

# P-2024 SERIES

VoIP ATA

## Support Notes

Version 3.60

Jul. 2007



**INDEX**

<b>Application Notes .....</b>	<b>5</b>
General Application Notes .....	5
Internet Connection.....	5
Using Dynamic DNS (DDNS).....	12
Using syslog.....	14
VoIP Application Notes.....	18
SIP Account Setup .....	18
Advanced Phone port settings.....	22
<b>FAQ .....</b>	<b>25</b>
ZyNOS FAQ .....	25
What is ZyNOS?.....	25
How to access the embedded web configurator?.....	25
What is the default LAN IP address and password? And, how do I change it?.....	25
How do I upload the firmware via the web configurator? .....	26
How do I upgrade/back up the firmware using an FTP client program through the LAN? .....	26
How do I upload or back up the configuration file (the ROM file) via the web configurator? .....	26
How do I back up/restore configurations using an FTP client program through the LAN? .....	27
Why can't I telnet into P-2024 from the WAN?.....	27
What should I do if I forget the system password?.....	27
What is SUA? When should I use SUA?.....	28
What is the difference between NAT and SUA?.....	28
How many network users does SUA/NAT support?.....	28
What are Device and Protocol filters? .....	29
Why can't I configure device or protocol filters? .....	29
Product FAQ .....	29
Will the P-2024 work with my Internet connection?.....	29
What do I need to use the P-2024? .....	29
What is PPPoE? .....	29
Does the P-2024 support PPPoE? .....	29
How do I know I am using PPPoE?.....	30
Why does my provider use PPPoE?.....	30

Which Internet Applications can I use with the P-2024?.....	30
How can I configure the P-2024? .....	30
What network interface does the P-2024 support? .....	30
What can I do with the P-2024?.....	30
Does the P-2024 support dynamic IP addressing?.....	30
What is the difference between the internal IP and the real IP from my ISP? .....	31
How does e-mail work through the P-2024? .....	31
What is the difference between the 'Standard' and 'RoadRunner' service?..	31
Is it possible to access a server running behind SUA from the outside Internet? If possible, how? .....	32
What DHCP capability does the P-2024 support? .....	32
How do I use the reset button? And which parameter will be reset by the reset button? .....	32
What network interface does the new P-2024 series support? .....	32
Does the P-2024 support TFTP? .....	32
Does the P-2024 support TFTP over WAN? .....	32
How fast is the DSL connection?.....	33
My P-2024 cannot obtain a WAN IP address from the ISP to connect to the Internet, what should I do?.....	33
What is DDNS?.....	36
When do I need the DDNS service? .....	36
What DDNS servers does the P-2024 support? .....	37
What is DDNS wildcard?.....	37
Does the P-2024 support DDNS wildcard? .....	37
VoIP FAQ .....	38
What is Voice over IP?.....	38
How does Voice over IP work? .....	38
Why use VoIP?.....	38
In addition, it would take a much longer time, more effort and money to implement new features using circuit switching. Since the IP technology is a standard and various applications are available, it is easier and more cost-effective to integrate new services and applications using IP. ....	38
What is the relationship between codec and VoIP? .....	38
What advantage does Voice over IP provide? .....	39
What is the difference between H.323 and SIP?.....	39
Can H.323 and SIP interoperate with each other? .....	39

What is voice quality?.....	39
How are voice quality normally rated?.....	39
What is codec? .....	39
What is the relationship between codec and VoIP? .....	40
What codec types does P-2024 support? .....	40
Which codec should I choose?.....	40
What do I need in order to use SIP? .....	40
I am unable to register to a SIP server .....	41
I can register to the SIP server but cannot establish a call.....	41
I can make or receive a call but the voice traffic only goes one way, not both way.....	41
I have tried all the troubleshooting steps, but still cannot register to the SIP server. What should I do next?.....	41
What should I do if there may be a hardware problem with my P-2024? ...	42
<b>Trouble Shooting.....</b>	<b>42</b>
Unable to Get WAN IP from ISP .....	42
Using Embedded Packet Trace .....	46
Debugging PPPoE Connection .....	61
<b>CLI Command List.....</b>	<b>72</b>

# Application Notes

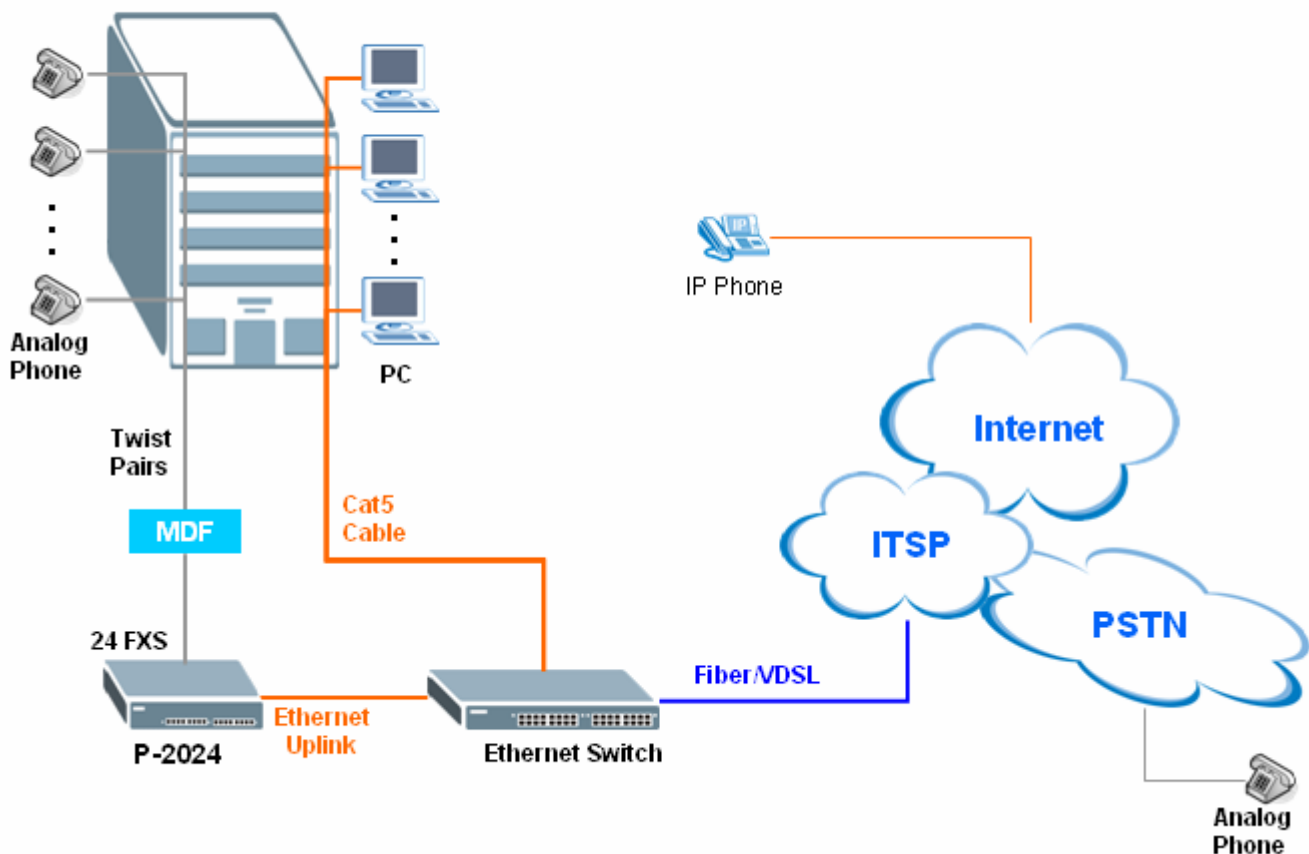
## General Application Notes

### Internet Connection

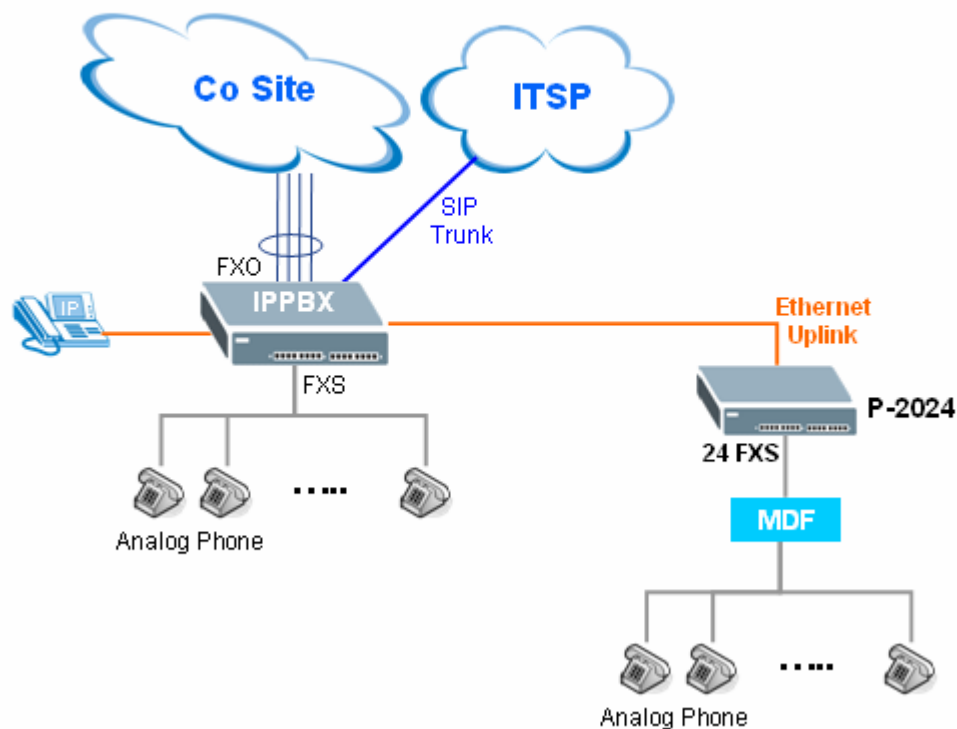
The following figures show a typical Internet access application using the P-2024. Before accessing the Internet in an office environment, you must configure the P-2024 as outlined below.

- Before you begin
- Setting up Your Windows Computer
- Setting up the P-2024
- Troubleshooting

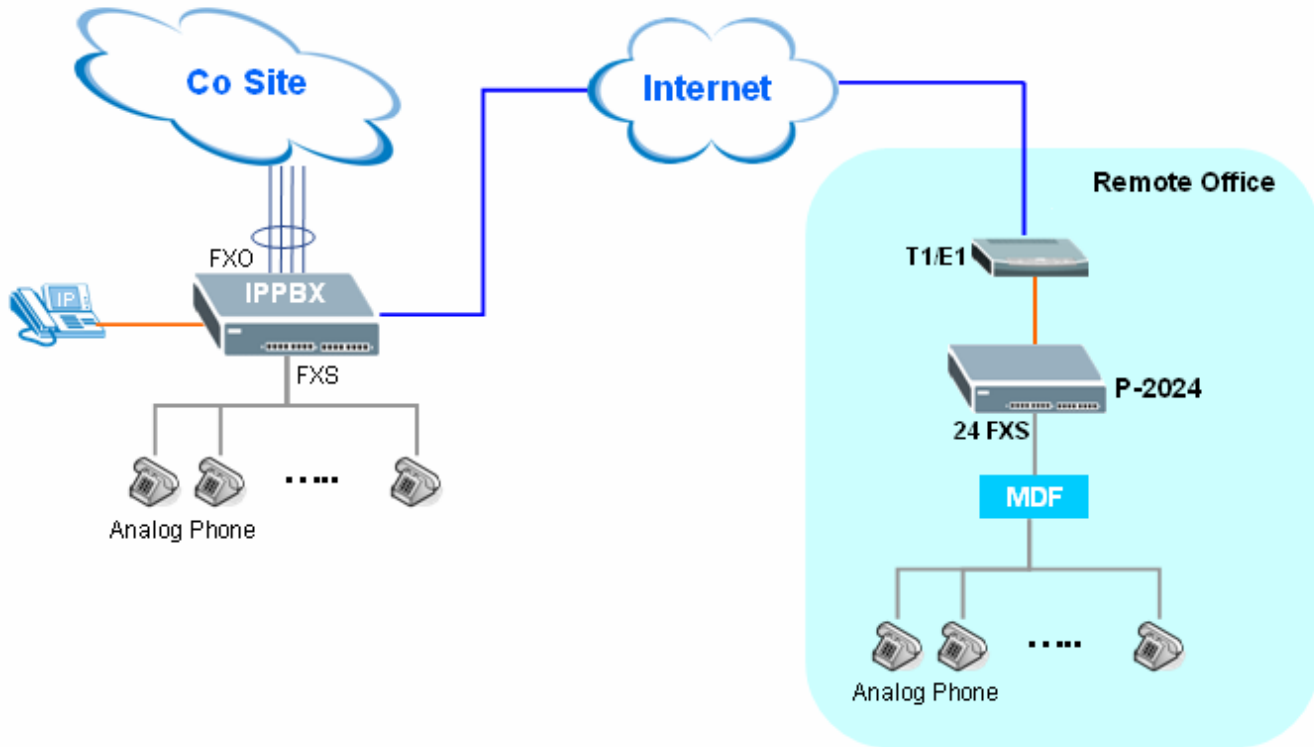
## Application – FTTB/VDSL



## Application – HQ Office IP PBX Extension



## Application – Remote Office VoIP Extension



- Before you begin

The following lists the default settings on the P-2024.

1. IP address = 192.168.5.1, subnet mask = 255.255.255.0 (24 bits)
2. Default SMT menu password = 1234

- Setting up your Windows computer(s)

### 1. Ethernet connection

Your computer(s) must have an Ethernet card installed.

- If you have only one computer, connect the computer to the LAN port on the P-2024 using a crossover Ethernet cable (red).
- If you have more than one computer, you must use a hub or switch to connect the computers to the LAN port on the P-2024 using a straight-through Ethernet cable.

## 2. TCP/IP Installation

You must first install TCP/IP software on each computer before you can use it for Internet access. If you have already installed TCP/IP, go to the next section to configure it; otherwise, follow these steps to install the software:

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** window, select **Protocol** and click **Add**.
- In the **Select Network Protocol** window, select **Microsoft** and then select **TCP/IP** from the **Network Protocols** field and click **OK**.

## 3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

- In the **Control Panel/Network** window, select **TCP/IP** and click **Properties**.
- In the **TCP/IP Properties** window, select **obtain an IP address automatically**.

Note: Do not assign arbitrary IP address and subnet mask to your computer(s). Otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
  - Click the **Gateway** tab. Select any installed gateways and click the **Remove** button until there is none listed.
  - Click the **DNS Configuration** tab and select **Disable DNS**.
  - Click **OK** to save and close the **TCP/IP** properties window
  - Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the computer. Make sure your P-2024 is turned on before clicking **Yes**. Repeat the above steps for each Windows computer on your network.
- **Setting up the P-2024**

If you have a Single User Account (SUA), follow the procedure to configure the P-2024. You can use a web browser (such as IE) to access the embedded web server on the P-2024 for device management. Before you can log into the web management interface, make sure that there is no one logging into the P-2024 through Telnet or the console port.

### 1. Accessing the P-2024 Web Management Interface



Open your web browser (such as IE) and enter the LAN IP address of the P-2024 in the Address field. The default LAN IP of the P-2024 is 192.168.5.1. Note that you can either enter <http://192.168.5.1> or <https://192.168.5.1> (for secure login).

## 2. First Login

A login screen displays. Enter the password and press Login. The default password is '1234' which is the same as the one you use to log into the SMT.



The image shows the login interface of a ZyXEL P-2024 router. At the top is a blue header with the ZyXEL logo. Below it, the text 'P-2024' is centered. The main area has a light blue gradient background. It says 'Welcome to your router Configuration Interface' and 'Enter your password and click "Login"'. There is a password field with a key icon and the text 'Password : ' followed by a white input box with four dots. Below the field, it says '( max. 30 alphanumeric, printable characters and no spaces )'. A yellow notepad icon is next to a 'Note:' section. The note says: 'Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.' At the bottom, there are two buttons: 'Login' and 'Reset'.

3. Use the **WIZARD SETUP** screens to configure Internet access settings on the P-2024.

http://192.168.5.1 - Welcome to ZyXEL P-2024... - Microsoft Internet Explorer 是由 ZyXEL 提供

## Connection Wizard

**STEP 1**   **STEP 2**

### System Information

**System Name**

Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.

**System Name:**

**Domain Name**

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below. This field is normally left blank.

**Domain Name:**

<Back   Next >   Exit

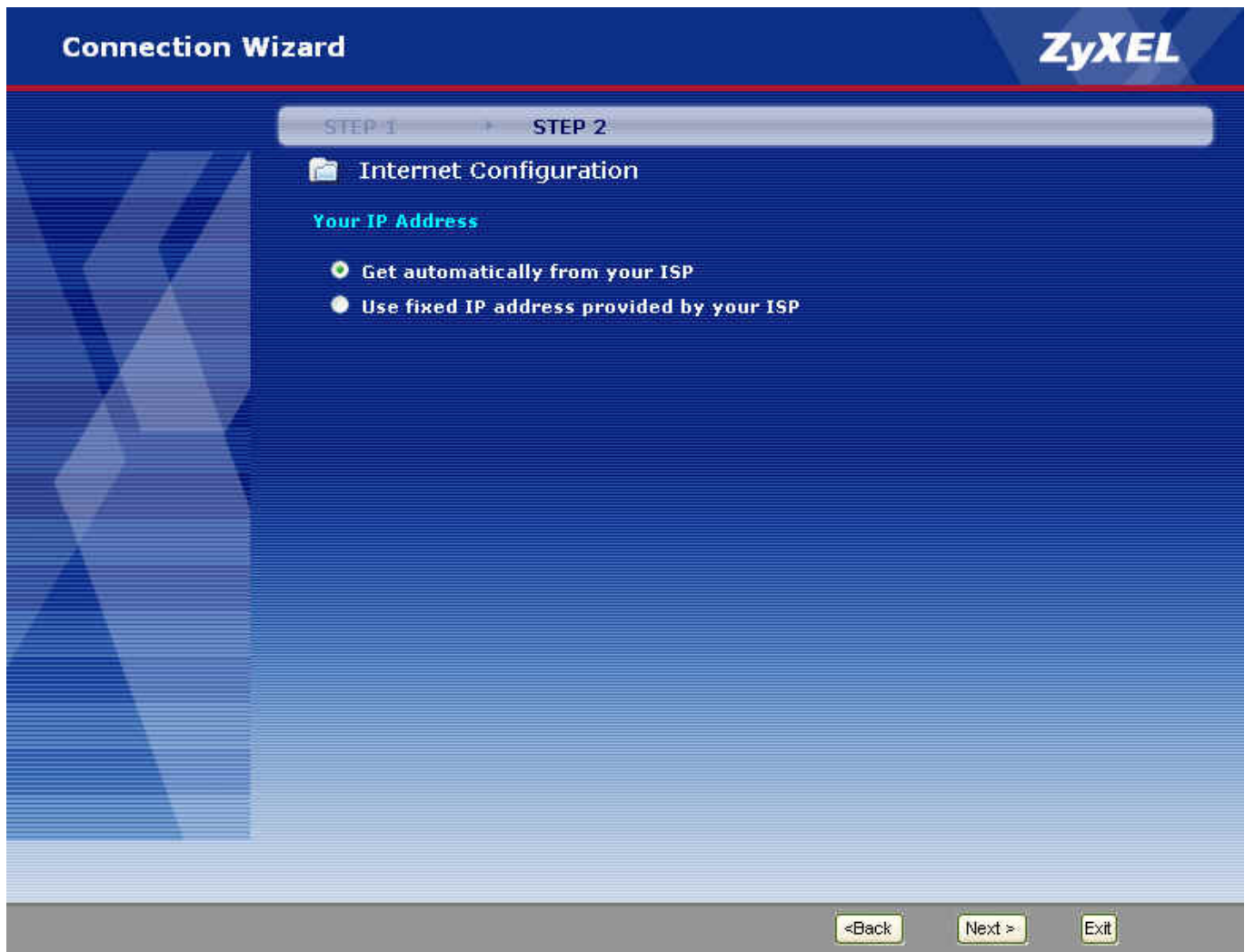
完成   網際網路

The Internet access configuration screen varies depending on the Internet connection type you select. The following figure shows an example screen for PPPoE connection type.

The image shows the ZyXEL Connection Wizard interface. At the top, it says "Connection Wizard" and "ZyXEL". Below this, there is a progress bar with "STEP 1" and "STEP 2". The current step is "STEP 2", which is titled "Internet Configuration". Under this title, it says "ISP Parameters for Internet Access". Below this, it says "Enter your Internet Service Provider's (ISP) connection settings." The form has four fields: "Connection Type" with a dropdown menu showing "PPP over Ethernet", "Service Name" with a text box containing "Any" and "(optional)" to its right, "User Name" with a text box containing "ZyXEL", and "Password" with a text box containing eight dots. At the bottom right, there are three buttons: "<Back", "Next >", and "Exit".

In the next wizard screen, select **Get dynamically from your ISP** if the ISP assigns you an IP address dynamically, otherwise select **Use Fixed IP address** and enter the static IP address given by ISP in the **MY**

WAN IP Address field.



---

## Using Dynamic DNS (DDNS)

### 1. What is DDNS?

A DNS (Domain Name Service) server stores the mappings of IP address and domain names. For example, when users enters a web site address (the domain name), the DNS server automatically maps the web site address to a public IP address and redirects the request to the intended web server.

Without DNS, users have to enter the IP address of the web server in order to access the web sites. This is very inconvenient and not user-friendly as users have to remember the IP addresses of the web sites.

However, if the web server is located behind the P-2024 which is using a dynamic WAN IP address, a fixed mapping cannot be stored in the DNS server database since the WAN IP address changes. Thus Dynamic DNS (DDNS) is used to solve this problem. For example, if you have hosted a web site (say [www.zyxel.com](http://www.zyxel.com)) on a server behind the P-2024 which is assigned a dynamic WAN IP address from the ISP, users can still access the web site from the WAN when you have set up the DDNS settings. With DDNS, users can always access a web site regardless of the WAN IP address on the P-2024.

When the ISP assigns the P-2024 a new WAN IP address, the P-2024 sends this information to the DDNS server which updates the IP-to-DNS mapping. Once the mapping is updated, outside users can still access the web site hosted on an internal server behind the P-2024.

You must register an account with a DDNS service provider. The DDNS server saves the password-protected e-mail address with the IP addresses and host names. Queries are serviced based on the e-mail addresses. Thus you must set the same e-mail address you used for DDNS in the P-2024 SMT menu 1.

Currently, the P-2024 supports [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) for the DDNS service. The following describes the setup procedure.

- Register an access with [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) DDNS service provider. You will be provided with a hostname for the internal server and a password for the IP address update on the DDNS server.
- Configure the DDNS settings on the P-2024. Log into the WEB GUI on the P-2024 and click **Maintenance > System > Dynamic DNS** to display the configuration screen as shown.

Maintenance > System > Dynamic DNS

General **Dynamic DNS** Time Setting

**Dynamic DNS Setup:**

☒ Enable Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name: [the local server's host name]

User Name:

Password:

☐ Enable Wildcard Option

☐ Enable off line option (Only applies to custom DNS)

**IP Address Update Policy:**

☐ Use WAN IP Address

☒ Dynamic DNS server auto detect IP Address

☐ Use specified IP Address: 0.0.0.0

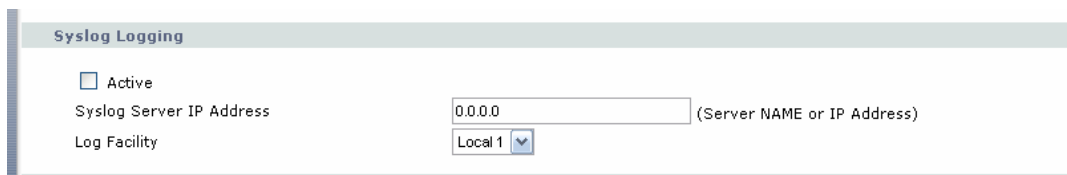
Apply Reset

Field Settings for DDNS:

Option	Description
<b>Service Provider</b>	Enter the DDNS server in this field. Currently the P-2024 supports <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> .
<b>Host</b>	Enter the hostname given by the DDNS service provider. For example, zyxel.com.tw.
<b>User</b>	Enter the user name that the DDNS service provider gives to your.
<b>Password</b>	Enter the password that the DDNS service provider gives to you.
<b>Enable Wildcard</b>	Enter the hostname for the wildcard function that the <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> supports. Note that the Wildcard option is available from the <a href="http://WWW.DYNDNS.ORG">WWW.DYNDNS.ORG</a> DDNS service provider.

## Using syslog

### 4. P-2024 Setup



**Syslog Logging**

☐ Active

Syslog Server IP Address:  (Server NAME or IP Address)

Log Facility:

Configuration:

1. **Active:** Select this check box to enable syslog logging.
2. **Syslog IP Address:** Enter the IP address of the syslog server that you wish to send the syslog.
3. **Log Facility:** Select a log location (numbered 1 to 7).

- **UNIX Setup**

1. Make sure that you start syslogd with the **-r** argument.

**-r** allows the syslog facility to receive messages from the network using an Internet domain socket with the syslog services. The default setting is NOT enabled.

2. Add the following commands at the end of the [/etc/syslog.conf](#) file.

```
local1.*                /var/log/zyxel.log
```

Where /var/log/zyxel.log is the full path of the log file.

3. Restart syslogd.

- **CDR log(call messages)**

Format:

```
sdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
```

String = board xx line xx channel xx, call xx, str

board = the hardware board ID

line = the WAN ID in a board

channel = channel ID within the WAN

call = the call reference number which starts from 1 and increments by 1 for each new call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

C01 Incoming Call xxxxBps xxxxx (L2TP,xxxxx is the Remote Call ID)

C01 Incoming Call xxxx (the connected speed) xxxxx (the Remote Call ID)

L02 Tunnel Connected(L2TP)

C02 OutCall Connected xxxx (the connected speed) xxxxx (the Remote Call ID)

C02 CLID call refused

L02 Call Terminated

C02 Call Terminated

Example:

```
Feb 14 16:57:17 192.168.5.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18, C01 Incoming Call OK
Feb 14 17:07:18 192.168.5.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18, C02 Call Terminated
```

- **Packet triggered log**

Format:

sdcmSyslogSend( SYSLOG\_PKTTRI, SYSLOG\_NOTICE, String );

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send 48 hexadecimal characters to the server

Example:

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
```

- **Filter log**

This message is available when the **'Log'** is enabled in the filter rule setting. The message consists of the packet header and the filter rules log contents.

Format:

sdcmSyslogSend(SYSLOG\_FILLOG, SYSLOG\_NOTICE, String );

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx]S04>R01mD



IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).

Src: Source Address

Dst: Destination Address

prot: Protocol (TCP,UDP,ICMP)

spo: Source port

dpo: Destination port

Example:

```
Jul 19 14:44:09 192.168.5.1 ZyXEL Communications Corp.: IP[Src=202.132.154.1 Dst=192.168.5.33 UDP  
spo=0035 dpo=05d4]]S03>R01mF  
Jul 19 14:44:13 192.168.5.1 ZyXEL Communications Corp.: IP[Src=192.168.5.33 Dst=202.132.154.1  
ICMP]]S03>R01mF
```

- **PPP Log**

Format:

sdcmdSyslogSend( SYSLOG\_PPPLOG, SYSLOG\_NOTICE, String );

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /IPXCP

Example:

```
Jul 19 11:43:25 192.168.5.1 ZyXEL Communications Corp.: ppp:LCP Starting  
Jul 19 11:43:29 192.168.5.1 ZyXEL Communications Corp.: ppp:IPCP Starting  
Jul 19 11:43:34 192.168.5.1 ZyXEL Communications Corp.: ppp:CCP Starting  
Jul 19 11:43:38 192.168.5.1 ZyXEL Communications Corp.: ppp:BACP Starting  
Jul 19 11:43:43 192.168.5.1 ZyXEL Communications Corp.: ppp:IPCP Opening  
Jul 19 11:43:51 192.168.5.1 ZyXEL Communications Corp.: ppp:CCP Opening  
Jul 19 11:43:55 192.168.5.1 ZyXEL Communications Corp.: ppp:BACP Opening  
Jul 19 11:44:00 192.168.5.1 ZyXEL Communications Corp.: ppp:LCP Closing  
Jul 19 11:44:05 192.168.5.1 ZyXEL Communications Corp.: ppp:IPCP Closing  
Jul 19 11:44:09 192.168.5.1 ZyXEL Communications Corp.: ppp:CCP Closing  
Jul 19 11:44:14 192.168.5.1 ZyXEL Communications Corp.: ppp:BACP Closing
```

## VoIP Application Notes

### SIP Account Setup

VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network.

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

The P-2024 supports up to two SIP accounts simultaneously. Follow the procedure below to configure SIP accounts on the device.

*Note:* You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configuring a SIP account on the P-2024.

The screenshot displays the ZyXEL P-2024 web interface. The left sidebar shows a navigation menu with 'Status', 'Network', 'VoIP', 'SIP', 'Phone', 'Phone Book', 'Management', and 'Maintenance'. The main content area is titled 'VoIP > SIP > SIP Settings'. It features two tabs: 'SIP Settings' (selected) and 'QoS'. The 'SIP Settings' tab contains the following configuration fields:

- SIP Account:** A dropdown menu set to 'SIP1'.
- SIP Settings Section:**
  - ☒ **Active SIP Account**
  - Number:** 799245
  - SIP Local Port:** 5060 (1025-65535)
  - SIP Server Address:** fwd.pulver.com
  - SIP Server Port:** 5060 (1-65535)
  - REGISTER Server Address:** fwd.pulver.com
  - REGISTER Server Port:** 5060 (1-65535)
  - SIP Service Domain:** fwd.pulver.com
  - ☒ **Send Caller ID**
- Authentication Section:**
  - User Name:** 799245
  - Password:** (masked with dots)

At the bottom of the configuration area are four buttons: 'Apply', 'Reset', 'Advanced Setup', and 'APPLY to ALL SIP'. The status bar at the bottom indicates 'Message Ready'.

After you have obtained the account information your ITSP provider provided, you can start configuring the SIP account.

**Step 1.** Log into the web configurator on the P-2024. Open a web browser and enter the management IP address (the default is 192.168.5.1) as the URL.

**Step 2.** A login screen displays. Enter the administrative login password (the default is 1234).

**Step 3.** In the main menu, click **VoIP > SIP** to display the **SIP Settings** screen. In the **SIP Account** drop-down list box, select a SIP account you want to configure.

**Step 4.** Select **Activate SIP Account** to enable this account and set the account information (such as **SIP number**, **SIP local port**, **SIP server address**, **SIP server port**, **Register server port**, **Register server address**, **SIP service domain**) in the fields below. Your ISP should provide you with the account information.

**Step 5.** Under **Authentication**, enter the account user name and password exactly as given by your ISP.

**Step 6.** Under **SIP Settings**, select **Send Caller ID** if you want to send the caller ID. Otherwise, clear the check box.

SIP Settings	
<input checked="" type="checkbox"/> Active SIP Account	
Number	799245
SIP Local Port	5060 (1025-65535)
SIP Server Address	fwd.pulver.com
SIP Server Port	5060 (1-65535)
REGISTER Server Address	fwd.pulver.com
REGISTER Server Port	5060 (1-65535)
SIP Service Domain	fwd.pulver.com
<input checked="" type="checkbox"/> Send Caller ID	

**Step 7.** You associate the SIP account to a specified phone port on the ZyXEL device. This allows you to set which phone(s) to use (ring) when an incoming call is received. In the WEB GUI, click **VoIP > Phone** to display the **Analog Phone** screen. Select a phone index number in the **Phone Port Settings** field and select which SIP account to use in the **Outgoing Call Use** section.

**Step 8.** Click on **Apply** to save the changes and make the settings take effect. If you want to configure the second SIP account, select **SIP2** in the **SIP Account** field and follow steps 1 – 7.

***Note:** If you associate both phone ports are associated with both SIP accounts, you cannot identify which account's incoming call is received.*

The following table describes the screen labels.

Label	Description
<b>SIP Account</b>	You can configure the P-2024 to use multiple SIP accounts. Select one to configure its settings on the P-2024.
<b>SIP Number</b>	<p>A SIP account's Uniform Resource Identifier (URI) identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. It is also known as a SIP identity or address. The format of a SIP identity is SIP-Number@SIP-Service-Domain.</p> <p>A SIP number is the part of the SIP URI that comes before the "@" symbol. Enter your SIP number in this field. You can use up to 31 ASCII characters.</p>
<b>SIP Local Port</b>	Use this field to configure the P-2024's listening port for SIP. Leave this

	field set to the default if you were not given a local port number for SIP.
<b>SIP Server Address</b>	Type the IP address of the SIP server in this field.
<b>SIP Server Port</b>	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a local port number for SIP.
<b>REGISTER Server Address</b>	<p>A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.</p> <p>Enter the SIP register server's address in this field.</p> <p><b>If you were not given a register server address, then enter the address from the SIP Server Address field again here.</b></p>
<b>REGISTER Server Port</b>	<p>Enter the SIP register server's listening port for SIP in this field.</p> <p><b>If you were not given a register server port, then enter the port from the SIP Server Port field again here.</b></p>
<b>SIP Service Domain</b>	<p>A SIP service domain is the domain name that comes after the @ symbol in a full SIP URI.</p> <p>Enter the SIP service domain name in this field. You can use up to 127 ASCII Extended set characters.</p>
<b>Authentication User ID</b>	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. Use ASCII characters.
<b>Authentication Password</b>	Type the password associated with the user name above. Use ASCII Extended set characters.
<b>Block Caller ID</b>	Select this check box to not show identification information when you make VoIP calls. Clear this check box to show identification information when you make VoIP calls.
<b>Apply to</b>	<b>Phone 1</b> and <b>Phone 2</b> correspond to the P-2024's physical <b>PHONE 1</b> and <b>2</b> ports, respectively. Select whether you want to receive calls for this SIP account on <b>Phone 1</b> , <b>Phone 2</b> or both. If you select both, you will not know

	which SIP account a call is coming in on.
<b>Advanced Settings</b>	Click <b>Settings</b> to open a screen where you can configure the P-2024's advanced VoIP settings like SIP server settings, the RTP port range and the coding type.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the P-2024.
<b>Reset</b>	Click <b>Reset</b> to begin configuring this screen afresh.

## Advanced Phone port settings

You can configure the ring/speaker volume and the echo cancellation settings for each phone port on the P-2024.

VoIP > Phone > Analog Phone > Advanced

Analog Phone 1

**Voice Volume Control**

Speaking Volume: -1(Min.)

Listening Volume: -1(Min.)

**Echo Cancellation**

☒ G.168 Active

**Others**

Dialing Interval Select: 3

☐ VAD Support

<Back Apply Reset

To configure advanced phone port setting, follow the steps below.

**Step 1.** Access the web configurator on the P-2024. In a web browser, enter the management IP address (the default is 192.168.5.1) of the P-2024 in the address bar.

**Step 2.** A login screen displays, enter the administrative login password (the default is 1234).

**Step 3.** In the navigation panel, click **VoIP > Phone > Analog Phone**.

**Step 4.** In the **Phone Port Settings** field, select which phone port you want to configure and click **Advanced Setup**.

**Step 5.** Set the phone port parameters and click **Apply** to save the settings and make the changes take effect. If you want to configure the second phone port, select **SIP2** in the **SIP Account** field and follow steps 1 – 5.

*The table below describes the related fields.*

Label	Description
<b>Phone Port Settings</b>	Use this field to select the phone port that you want to configure.
<b>Speaking Volume</b>	Use this field to set the loudness that the P-2024 uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
<b>Listening Volume</b>	Use this field to set the loudness that the P-2024 uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.
<b>Outgoing Call use</b>	<b>SIP 1</b> and <b>SIP 2</b> correspond to the P-2024's SIP accounts. Select whether you want the phone(s) attached to this phone port to use SIP account 1, 2 or both when you make a call. If you select both SIP accounts, the P-2024 will first try to use SIP account 2 and then SIP account 1 when you make a call.
<b>G.168 Active</b>	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
<b>VAD Support</b>	Select this check box to use Voice Activity Detection (VAD) to reduce the bandwidth that a call uses. The P-2024 will generate and send comfort noise when you are not talking.
<b>Dialing Interval</b>	When you are dialing a telephone number the P-2024 waits this long after you stop pressing the buttons before initiating the call. Select how many seconds you want the P-2024 to wait after the last input on the telephone's keypad before dialing (making) a call.
<b>Apply</b>	Click <b>Apply</b> to save your changes back to the P-2024.
<b>Reset</b>	Click <b>Reset</b> to begin configuring this screen afresh.

Step 6. Click **Add** to save the entry to the phone book.

*Each field's detail description of the page is listed below.*

Label	Description
<b>Add New Entry</b>	Use this section of the screen to edit and save new or existing speed dial phone book entries.
<b>Speed Dial</b>	Select a speed dial key combination from the drop-down list box.
<b>SIP Number</b>	Enter the SIP number of the party that you will call (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
<b>Name</b>	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
<b>Type</b>	<p>Select <b>Use Proxy</b> if calls to this party use your SIP account configured in the VoIP screen.</p> <p>Select <b>Non-Proxy (Use IP or URL)</b> if calls to this party use a different SIP server or go directly to the callee's VoIP phone (IP-to-IP). Enter the SIP server's or the party's IP address or domain name (up to 127 ASCII Extended set characters).</p>
<b>Add</b>	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the <b>Speed Dial Phone Book</b> section of the screen.
<b>Speed Dial Phone Book</b>	This section of the screen displays the currently saved speed dial entries. You can configure up to 10 entries and use them to make calls.
<b>Speed Dial</b>	This is the entry's speed dial key combination. Press this key combination on a telephone attached to the P-2024 in order to call the party named in this entry.
<b>Name</b>	This is the descriptive name of the party that you will use this speed dial entry to call.
<b>SIP Number</b>	This is the SIP number of the party that you will call.
<b>Type</b>	This field displays <b>Use Proxy</b> if calls to this party use one of your SIP accounts. This field displays the SIP server's or the party's IP address or domain name if calls to this party do not use one of your SIP accounts.



<b>Delete</b>	Click this button to remove an entry from the speed dial phonebook.
<b>Edit</b>	Click this button to change the speed dial entry. The speed dial entry displays in the <b>Add New Entry</b> section of the screen where you can edit it.
<b>Clear</b>	Click this button to remove all of the entries from the speed dial phonebook.

---

## FAQ

### ZyNOS FAQ

#### What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all P-2024 ATAs that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites and public download web site as they become available.

#### How to access the embedded web configurator?

The web configurator is a user friendly configuration interface via a web browser. You can access the web configurator by entering the LAN IP address of the P-2024 in the web browser. The default the P-2024 LAN IP is 192.168.5.1. Your computer IP address must be in the same subnet (or range) as the P-2024' s LAN IP address.

#### What is the default LAN IP address and password? And, how do I change it?

The default LAN IP address is "192.168.5.1" and you can change the LAN IP in web configuration (click LAN > LAN TCP/IP). The default login password is 1234. After you have successfully logged into the web configuration, you can change the password in the Password screen (click SYSTEM > Password. In the

Password screen, enter the old password and the new password and the new password again to confirm. Click Apply to save the changes.

### **How do I upload the firmware via the web configurator?**

Follow the procedure below to update the device firmware via the web configurator.

- a. Log into the web configurator.
- b. In the navigation panel, click MAINTENANCE.
- c. Click the F/W Upload tab.
- d. Click Browse and locate the directory of the firmware you want to upload and click Upload.
- e. A message displays indicating that the firmware is successfully updated and that the P-2024 will reboot.

### **How do I upgrade/back up the firmware using an FTP client program through the LAN?**

You can use an FTP program to transfer files (firmware or configuration files) to or from the P-2024. Follow the procedure below to upload the firmware to a device using FTP.

- a. Use an FTP program to put the firmware file (rename as “ras” ) on the P-2024. After the file transfer is complete, the P-2024 stores the uploaded firmware to its FLASH ROM and reboots.  
Note: Do NOT turn off the device while the file transfer process is in progress. Doing so will damage your device and render it useless. Wait until the system LED turns steady before accessing the device.
- b. To backup your firmware, use the FTP client program to get the ‘ras’ file from the P-2024.

### **How do I upload or back up the configuration file (the ROM file) via the web configurator?**

You can upload a configuration file to restore the device to the previously saved configuration, or reset the device to the factory defaults.

Follow the procedure below to upload a configuration file via the web configurator.

- a. Log into the web configurator.
- b. In the navigation panel, click MAINTENANCE.
- c. Click the Configuration tab.

- d. Click the Restore tab and click Browse to locate the directory of the configuration file you want to upload.
- e. Click Upload.

Follow the procedure below to back up the configuration file from the device via the web configurator.

- a. Log on into the web configurator.
- b. In the navigation panel, click MAINTENANCE.
- c. Click the Configuration tab.
- d. Click Backup. A screen displays prompting you to specify a location to store the configuration file.
- e. Click Save file and browse to where you want the file to be saved.
- f. Click Save.

### **How do I back up/restore configurations using an FTP client program through the LAN?**

- a. Use an FTP client program in your computer (such as the Cuteftp or wsftp client) to log into your P-2024.
- b. To back up current device configuration, use the FTP client program to get the 'rom-0' file from the P-2024.
- c. To restore device configuration, use the FTP client program to put a configuration file (rename to ROM-0) on the P-2024.

### **Why can't I telnet into P-2024 from the WAN?**

The following lists the possible reasons why you cannot telnet into the P-2024 from the WAN.

- a. You did not enable the Telnet service on WAN interface for remote management in SMT menu 24.11.
- b. Telnet service is enabled but your computer IP address is not included in the secured host list in SMT menu 24.11. In this case, you will see the 'Client IP is not allowed!' error message in the Telnet screen.
- c. The default filter rule 3 (Telnet\_FTP\_WAN) is applied in the Input Protocol field in SMT menu 11.5. This blocks access from the WAN.

### **What should I do if I forget the system password?**

In case you forget the system password. You can reset the unit back to the factory defaults. You can do this by using a sharp pointed object (such as a pen) to press and hold down the Reset button for 5 seconds or until the power LED starts to blink, then release. The unit is reset back to the factory defaults. The reset button is located near the power jack on the unit's back panel.

*Note: Resetting the unit back to the factory defaults erases all your previous settings.*

## **What is SUA? When should I use SUA?**

SUA (Single User Account) is a unique feature supported by the P-2024 to allow more than one person to access the Internet concurrently for the cost of a single user account.

When P-2024 acting as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputed the appropriate header checksums and forwards the packet to the Internet as if it originated from the P-2024 using the WAN IP address assigned by the ISP. When reply packets from the Internet are received by the P-2024, the original IP source address and TCP/UDP source port numbers are written back into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its intended destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

## **What is the difference between NAT and SUA?**

NAT is a generic name defined in RFC 1631 'The IP Network Address Translator (NAT)'. SUA (Internet Single User Account) is ZyXEL's proprietary implementation and trade name for the PAT feature which is a specific type of NAT. SUA (or PAT for NAT) translates address into port mapping.

The primary motivation for RFC 1631 is that there is not enough IP address to go around. In addition, many corporations simply did not bother to obtain legal (globally unique) IP addresses for their networks and now finding themselves unable to connect to the Internet.

Basically, NAT is the process of translating one address to another. A NAT implementation can be as simple as substituting an IP address with another. This allows a network to solve the illegal address problem mentioned above without going through each and every host.

The goal of ZyXEL's SUA is to minimize the Internet access cost in a small office environment by using a single IP address to represent multiple hosts on the LAN. It does more than IP address translation, so that multiple hosts on the LAN can access the Internet at the same time.

## **How many network users does SUA/NAT support?**

The P-2024 does not limit the number of the users but the number of the sessions for Internet access. The P-2024 supports 1024 sessions. You can view the current active sessions using the 'ip nat iface enif0 disp' command in SMT menu 24.8.

## **What are Device and Protocol filters?**

In ZyNOS, there are two filter groups: device filter and protocol filter. Generic filters belong to the device filter group while TCP/IP and IPX filters belong to the protocol filter group.

## **Why can't I configure device or protocol filters?**

In ZyNOS, you cannot configure device filters and protocol filters in the same filter set.

---

## **Product FAQ**

### **Will the P-2024 work with my Internet connection?**

The P-2024 is designed to work with cable and ADSL modems. The P-2024 comes with an Ethernet port to connect to your computer so the P-2024 is placed between your computer and your modem. The P-2024 also supports PPPoE Internet connection type.

### **What do I need to use the P-2024?**

Ethernet ports for LAN and WAN connection. You should connect the computer to the LAN port and the external modem to the WAN port. If the ISP uses PPPoE or Roadrunner Authentication, you need the user account to enter in the P-2024.

### **What is PPPoE?**

PPPoE (Point-to-Point Protocol over Ethernet) is an IETF draft standard specifying how a computer interacts with a broadband modem (such as xDSL, cable, wireless, etc.) to access the high-speed data networks via a PPP dialer (such as Microsoft's Dial-Up Networking). PPPoE supports a broad range of applications and services including authentication, accounting, secure access and configuration management. Some ISPs still provides PPPoE connection type today. Before configuring PPPoE in the P-2024, make sure your ISP supports PPPoE.

### **Does the P-2024 support PPPoE?**

Yes. The P-2024 has already supported PPPoE since ZyNOS 2.50.

**How do I know I am using PPPoE?**

PPPoE requires a user account to log into the service provider's server. If you need to configure a user name and password on your computer to connect to the ISP, you are probably using PPPoE. If you connect to the Internet when you turn on your computer, you probably are not using PPPoE. You can also check with your ISP or the information sheet given by the ISP. Choose PPPoE as the encapsulation type in the P-2024 if the ISP uses PPPoE.

**Why does my provider use PPPoE?**

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and services including authentication, accounting, secure access and configuration management.

**Which Internet Applications can I use with the P-2024?**

The P-2024 supports most common applications including MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, QuakeII, QuakeIII, StarCraft, and Quick Time.

**How can I configure the P-2024?**

- a. Telnet remote management- Menu driven user interface for easy remote management
- b. Web browser- embedded web server for easy configuration

**What network interface does the P-2024 support?**

The P-2024 comes with a 10/100M Ethernet interface to connect to your LAN computer and the external cable/DSL modem.

**What can I do with the P-2024?**

You can connect to the Internet through the P-2024. This allows you to browse the web, send and receive e-mail, and download/share files. These are just a few of many benefits you get when you put the whole office on-line with the P-2024 Internet Access Sharing ATA.

**Does the P-2024 support dynamic IP addressing?**

Yes. You can set the P-2024 to use a static WAN IP address or set it to use a dynamic IP address from the ISP.

**What is the difference between the internal IP and the real IP from my ISP?**

Internal IP addresses are also referred to as virtual IP addresses. They are a group of up to 255 IP addresses that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP address (or the public IP address) you obtain from the ISP, instead, can be recognized or pinged by other real IP addresses. The P-2024 Internet Access Sharing ATA works like an intelligent ATA that routes network traffic between the virtual IP addresses and real IP addresses.

**How does e-mail work through the P-2024?**

It depends on what kind of IP address you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through the P-2024 using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access rights.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address.

Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through the P-2024 using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access rights.

**What is the difference between the 'Standard' and 'RoadRunner' service?**

The [Road Runner](#) service is commonly used in the USA and it requires the user to "log in" to the service provider network before Internet access is allowed. The most popular implementation is TAS (Toshiba Authentication System) with a packet filtering firewall in the upstream direction. Before users are logged in, they can send ICMP packets (that is, ping) to a remote host through the Internet. However, all outgoing (upstream) TCP and UDP packets to the Internet are blocked. Thus users can access the local local DNS/login server. Downstream packets (or packets from the Internet to the users) are not filtered or blocked.

With [Standard](#) service, no user login is required. This is commonly used with a cable modem. The P-2024 supports both [Road Runner and Standard](#) services in SMT menu 4 for connecting to the ISPs for Internet connection.

**Is it possible to access a server running behind SUA from the outside Internet? If possible, how?**

Yes, it is possible because P-2024 delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in SMT Menu 15 - [SUA Server Setup](#).

**What DHCP capability does the P-2024 support?**

The P-2024 supports DHCP client on the WAN port. The P-2024's DHCP client allows it to get a public WAN IP address from the ISP automatically if your ISP uses DHCP as a method to assign IP addresses.

**How do I use the reset button? And which parameter will be reset by the reset button?**

Use a sharp pointed object to press the reset button located near the power connector. Press and hold down the button for about five seconds to reset the device. All device settings, including the login password and IP address, will be reset to the factory defaults.

The default IP address is 192.168.5.1 and the default login password is 1234.

**What network interface does the new P-2024 series support?**

The new P-2024 series comes with an auto MDX/MDIX 10/100M Ethernet LAN port to connect to computer(s) or switch(es) on the LAN and one 10/100M Ethernet port to connect to the external cable/DSL modem on the WAN.

---

**Does the P-2024 support TFTP?**

Yes. In addition to the direct console port connection, the P-2024 supports firmware upload and configuration file uploading/download using TFTP (Trivial File Transfer Protocol) over LAN.

**Does the P-2024 support TFTP over WAN?**

Although TFTP also works over the WAN, it is not recommended because of potential data corruption error while transferring files to the P-2024.

How can I upload data to outside Internet over the one-way cable?



Set up an alternate path for connection to the Internet (for example, a dialup connection). You can still receive downstream packets from the Internet through the P-2024.

### **How fast is the DSL connection?**

There are a number of factors that can affect the speed of your ADSL connection. The connection speed may depend on how fast your computer handles data, how fast data can be transmitted between your computer and the modem, how well the cable modem handles traffic during network congestion, or how much bandwidth is provided by the ISP, etc.

Depending on your computer, data process speed varies and few computers can achieve data processing rates at up to 30 Mbps.

Ethernet (10baseT) is the most popular cable modem interface standard for a computer. This automatically limits the speed of the connection to less than 10 Mbps even if the modem can receive at 30 Mbps. Most Local Area Networks use 10baseT Ethernet, and although they are 10 Mbps networks, it takes a much longer than one second to transmit 10 megabits (or 1.25 megabytes) of data from one terminal to another.

Cable modems on the same node share the same bandwidth, which means that congestion is created when too many people try to access the Internet at the same time. In addition, when one user is downloading large graphic or video files, a significant portion of the shared bandwidth is used thus slowing down access for other users in the same neighborhood.

Most independent Internet Service Providers today connect to the Internet using a single 1.5 Mbps "T1" telephone line. All their subscribers share that 1.5 Mbps bandwidth. Cable companies connecting to the Internet backbone using a T1 limit their subscribers to an absolute maximum of 1.5 Mbps.

To create the appearance of faster network access, ISPs store or "cache" frequently requested web sites and Usenet newsgroups on a server in the central office (CO). Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? Theoretically, they can receive data at speeds up to 30 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall to about 1.5 Mbps.

### **My P-2024 cannot obtain a WAN IP address from the ISP to connect to the Internet, what should I do?**

There are various ways your ISP controls user access and login. Once a user has successfully logged into, the ISP will provide the WAN IP address to the user.

The following lists the methods ISP' s authenticates users.

1. Check if the modem' s MAC address' is valid.
2. Check if the host name is correct. The host name is usually the text after the @ sign. For example, @home
3. Check if the user ID is valid. This is commonly used with the RR-Toshiba Authentication and RR-Manager Authentication services.

If you are not able to get a WAN IP address from your ISP, check which authentication method your ISP uses and configure the settings on the P-2024. The following sections describe how you can solve this problem.

### 1. If your ISP checks the MAC address

Some ISPs checks the user device (usually a computer) MAC address before assigning a WAN IP address. If the MAC address matches one on the ISP' s system, the ISP sends an IP address to the user device and allows Internet access. However, if the user connects another computer with a different MAC address directly to the modem, the ISP discards any DHCP discovery packets from the un-authorized MAC address and no IP address is assigned.

You can set the P-2024 to copy the MAC address of the computer whose MAC address is authorized by the ISP. The P-2024 will use the copied MAC address as its WAN MAC address.

In SMT menu 2, enter the computer MAC address. The P-2024 will use the copied MAC address as its WAN MAC address and update SMT menu 24.1.

MAC Address:

Assigned By= **IP address attached on LAN**

IP Address= **192.168.5.33**

Field settings:

- a. Assigned By: Select **IP address attached on LAN**.
- b. IP Address: Enter the IP address of the computer whose MAC address is authorized by the ISP.

### 2. If your ISP checks the host name

Some ISPs check the host name information contained in the DHCP request sent by the user computer. A host name is text that comes after the @ sign. For example, in account@home.com, the host name is "home.com". If a technician from your ISP helped you set up Internet connection, he/she set the host name as the computer name on your computer (in the Networking screen). When you connect that computer to the P-2024, you must set the same name as the P-2024's system name in SMT menu 1.

Menu 1 - General Setup

System Name= zyxel

Field Setting:

- System Name: Enter the same name as the computer.

### 3. If your ISP checks the User ID

This authentication method is used mostly by ISPs providing RoadRunner services (for example, RR-TAS (Toshiba Authentication Service) or RR-Manager authentication). You must configure the service type, username and password exactly as provided by your ISP in SMT menu 4.

Menu 4 - Internet Access Setup

ISP's Name= MyISP

Encapsulation= Ethernet

Service Type= **RR-Toshiba**

My Login= cso@zyxel

My Password= \*\*\*\*\*

Retype to Confirm= N/A

Login Server= **0.0.0.0**

IP Address Assignment= Dynamic

IP Address= N/A

IP Subnet Mask= N/A

Gateway IP Address= N/A  
Network Address Translation= SUA Only

Field settings:

- a. **Service Type:** Select **RR-TAS** or **RR-Manager** authentication method used by your ISP.
- b. **Login Server:** Enter the IP address of the authentication server if you know it. Otherwise, leave this field to the default to have the P-2024 automatically obtain this information.
- c. **My Login Name:** Enter the login user name given to you by your ISP
- d. **My Password:** Enter the password associated with the login name.
- e. **WAN IP Address Assignment:** If the ISP did not assign you a fixed (or static) WAN IP address, select **Dynamic**, otherwise, select **Static**.
- f. **IP Address, Subnet Mask, Gateway IP Address:** If you select **Static** in the **WAN IP Address Assignment** field, enter the IP address, subnet mask and gateway device IP address provided by your ISP.

## What is DDNS?

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname, allowing your computer to be more easily assessable from various locations on the Internet. To use the service, you must first apply an account from one of the several free DDNS service providers such as [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG).

Without DDNS, you have to tell your users the WAN IP address of your server for them to access. It is inconvenient for the users if this IP is dynamic which changes. With DDNS supported on the P-2024, you use a DNS name (e.g., [www.zyxel.com.tw](http://www.zyxel.com.tw)) supplied by the DDNS service provider to your server (e.g., Web server). Outside users can always access the web server at [www.zyxel.com.tw](http://www.zyxel.com.tw) regardless of whether the WAN IP on the P-2024 is dynamic or static.

When the ISP assigns the P-2024 a new IP address, the P-2024 updates this IP address to the DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., [www.zyxel.com.tw](http://www.zyxel.com.tw)) is still easily accessible.

## When do I need the DDNS service?

When you want your internal server to be accessible by using DNS name rather than using a dynamic IP address, use the DDNS service. The DDNS server maps a dynamic IP address to a static hostname. Whenever

the ISP assigns you a new IP address, the P-2024 sends this IP address to the DDNS server to update its IP-DNS table.

### **What DDNS servers does the P-2024 support?**

Currently, the P-2024 supports [WWW.DYNDNS.ORG](http://WWW.DYNDNS.ORG) for DDNS service. This is the web site to which you apply the DNS and update the P-2024 WAN IP.

### **What is DDNS wildcard?**

Some DDNS servers support the wildcard feature which allows the \*.yourhost.dyndns.org hostname to be mapped to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple internal servers and you want users to be able to use addresses such as www.yourhost.dyndns.org and still reach your server.

### **Does the P-2024 support DDNS wildcard?**

Yes. the P-2024 supports DDNS wildcard that [WWW.DynDNS.ORG](http://WWW.DynDNS.ORG) supports. To use wildcard, simply enter yourhost.dyndns.org in the **Host** field in SMT menu 1.1.

## VoIP FAQ

### **What is Voice over IP?**

Voice over IP (VoIP) is an emerging technology based on the open IEEE standards. VoIP refers to the transmission of voice data over the Internet. Various protocols are available for voice transport. The most commonly used are SIP and H.323.

Voice over IP (VoIP) is an emerging technology based on open IEEE standards. VoIP refers to the transmission of voice data over the Internet. Various protocols are available for voice transport. The most commonly used are SIP and H.323.

### **How does Voice over IP work?**

In VoIP, voice data is sent digitally in discrete packets through the Internet, not through the traditional circuit switch of PSTN. To do so, an analog-to-digital converter is required at sender side to translate voice (analog signal) to digital signal before transmission. At the receiver end, an analog-to-digital converter converts the digital signal back to analog so the voice can be heard on the phone.

### **Why use VoIP?**

Traditionally voice data is transmitted using circuit switching. Since circuit switching is designed to carry voice, it does it very well. However, as broadband networks become a mainstream for network access and technologies have evolved, we don't want to confine ourselves to just using text-based applications (such as e-mail, instant messaging, etc.) for communication over the Internet. Thus, the convenience of voice communication through the Internet has quickly become popular.

**In addition, it would take a much longer time, more effort and money to implement new features using circuit switching. Since the IP technology is a standard and various applications are available, it is easier and more cost-effective to integrate new services and applications using IP.**

### **What is the relationship between codec and VoIP?**

In order to send voice (analog signal) over IP, it first needs to be digitized. Codec is a technique used to digitize analog signal into digital signals and vice versa. There are various speech codec available for VoIP. Each codec has its advantages and disadvantages.

**What advantage does Voice over IP provide?**

VoIP provides advanced integration of text, video and voice in emails. This cannot be done using traditional circuit switching (PSTN).

**What is the difference between H.323 and SIP?**

H.323 and SIP are proposed by different groups. Session Initiation Protocol (SIP) is a standard introduced by the Internet Engineering Task Force in 1999 to carry voice over IP. Since it was created by the IETF, it approaches voice and multimedia from the Internet, or IP. Whereas H.323 emerged around 1996, and as an International Telecommunication Union standard, it was designed from a telecommunications perspective. Both standards have the same objective - to enable voice and multimedia convergence with IP protocols.

**Can H.323 and SIP interoperate with each other?**

In interoperability between the two, the industry is making slow but sure progress. Interoperability must first happen between vendor implementations of the same protocol (SIP-to-SIP and H.323-to-H.323) and then between protocols. Currently in order for SIP client to talk to H.323 client the ITSP must have a trunking gateway act as a translator between the two protocols without the trunking gateway the two protocols are not able to communicate to one another.

**What is voice quality?**

Voice quality is how well a person can hear the voice on the opposite end.

**How are voice quality normally rated?**

Voice quality is most commonly rated through a voice quality metric called the Mean Opinion Score (MOS) which is recommendation by ITU-T. The MOS is a 5-point scale where 5 represent excellent voice quality and 1 represent bad voice quality.

**What is codec?**

Codec is an algorithm that converts analog signal into digital signal and vice versa. There are three codeec types: waveform, source, and hybrid codec. Each consume different amount of bandwidth and provide different voice quality.

## **What is the relationship between codec and VoIP?**

VoIP is the general term to refer to the sending of digitized voice information in discrete packets over public digital network (the Internet) where other data packets can be sent at the same time. A codec determines how much bandwidth voice packets will use. To save bandwidth usage, you would use as little bandwidth as possible at the cost of reduced voice quality.

## **What codec types does P-2024 support?**

The P-2024 supports the following commonly used codecs.

- G.726
- G.729 a/b voice codec
- G.711u-law voice codec
- G.711a-law voice codec
- G.723.\* (Option)

## **Which codec should I choose?**

Choose a codec that is also supported on the remote VoIP host since both ends of the VoIP connection must use the same codec. In general, a codec with low bandwidth consumption and high voice quality is a good codec.

## **What do I need in order to use SIP?**

The following lists the minimum requirement for running VoIP applications.

1. A high-speed Internet connection. You can connect to the Internet using a cable or DSL modem. Or subscribe to high-speed network services such as ISDN, DSL or T-1. The bandwidth requirement varies depending on the amount of traffic in your network.
2. A PC with VoIP software installed or an external VoIP gateway (such as an ATA or the P-2024 2602 VoIP station ATA).
3. An account from a VoIP services provider (such as an ITSP). The account can be configured to recognize your calls automatically, or you can require the users to enter their assigned unique account numbers.



**I am unable to register to a SIP server**

If you are unable to register to a SIP server, do the following.

1. Make sure the Internet connection is up and that you are able to ping the SIP register server from the LAN behind the P-2024. If your register server uses a domain name, make sure DNS name can be resolved. If you are using a static WAN IP address, make sure the DNS server is configured correctly on your P-2024.
2. Make sure the SIP account is correct and the password is entered correctly. They may be case-sensitive.
3. Check if there is a NAT ATA install before the P-2024 which is a VoIP station gateway. It is NOT recommended that you install a NAT ATA in front of the P-2024 as this may cause unexpected problems. If you still want to install a NAT ATA, use a VoIP ATA (VoIP Analog Telephone Adapter), such as the P-2024 ATA series, instead.

**I can register to the SIP server but cannot establish a call**

If you are able to register to the SIP server but cannot make a call through the P-2024, it is very likely there a NAT ATA or a firewall blocks the traffic.

It is NOT recommended that you install a NAT ATA in front of the P-2024 as this may cause unexpected problems. If you still want to install a NAT ATA, use a VoIP ATA (VoIP Analog Telephone Adapter), such as the P-2024 ATA series, instead.

**I can make or receive a call but the voice traffic only goes one way, not both way**

If you can register to a server and can only make an out- going call but cannot receive incoming calls or the incoming call signal establishment can be made but the voice traffic only goes one way, there is very likely a NAT/firewall ATA installed before the P-2024. Refer to the NAT/firewall related questions for more information.

**I have tried all the troubleshooting steps, but still cannot register to the SIP server. What should I do next?**

In this case, contact your local service provider for support. If they cannot solve your problem, they will send your problem to the ZyXEL global technical support center. To help out the problem they will escalate your problem to ZyXEL tech center.

To help us solve your problem quickly, please prepared the following information.

1. Serial number of the device.
2. SIP Call server type and service provider.
3. Your device firmware version and romfile (or the configuration file) with the administrator login password.
4. Detail information of what you have tried to resolve the problem.

**What should I do if there may be a hardware problem with my P-2024?**

Refer to the troubleshooting section in the user's guide for basic hardware troubleshooting and diagnostic tips. If the hardware problem persists after you have followed the User's Guide to remedy the problem, contact your ZyXEL local vendor and send the device in for service (with an RMA number).

---

## Trouble Shooting

### Unable to Get WAN IP from ISP

**My P-2024 cannot obtain an IP address from the ISP for Internet access, what should I do?**

---

There are various ways your ISP controls user access and login. Once a user has successfully logged into, the ISP will provide the WAN IP address to the user.

The following lists the methods ISP's authenticates users.

4. Check if the modem's MAC address' is valid.
5. Check if the host name is correct. The host name is usually the text after the @ sign. For example, @home
6. Check if the user ID is valid. This is commonly used with the RR-Toshiba Authentication and RR-Manager Authentication services.

If you are not able to get a WAN IP address from your ISP, check which authentication method your ISP uses and configure the settings on the P-2024. The following sections describe how you can solve this problem.

## 1. If your ISP checks the MAC address

Some ISPs check the user device (usually a computer) MAC address before assigning a WAN IP address. If the MAC address matches one on the ISP's system, the ISP sends an IP address to the user device and allows Internet access. However, if the user connects another computer with a different MAC address directly to the modem, the ISP discards any DHCP discovery packets from the un-authorized MAC address and no IP address is assigned.

You can set the P-2024 to copy the MAC address of the computer whose MAC address is authorized by the ISP. The P-2024 will use the copied MAC address as its WAN MAC address.

In SMT menu 2, enter the computer MAC address. The P-2024 will use the copied MAC address as its WAN MAC address and update SMT menu 24.1.

Menu 2 - WAN Setup
MAC Address:
Assigned By= IP address attached on LAN
IP Address= 192.168.5.33

Field settings:

- Assigned By=, Select **IP address attached on LAN**.
- IP Address=, Enter the IP address of the computer whose MAC address is authorized by the ISP.

---

## 2. If your ISP checks the Host Name

Some ISPs check the host name information contained in the DHCP request sent by the user computer. A host name is text that comes after the @ sign. For example, in account@home.com, the host name is "home.com". If a technician from your ISP helped you set up Internet connection, he/she set the host name as the computer

name on your computer (in the Networking screen). When you connect that computer to the P-2024, you must set the same name as the P-2024's system name in SMT menu 1.

Menu 1 - General Setup

System Name= zyxel

Domain Name=

First System DNS Server= From ISP

IP Address= N/A

Second System DNS Server= From ISP

IP Address= N/A

Third System DNS Server= From ISP

IP Address= N/A

Edit Dynamic DNS= No

Field Setting:

- System Name: Enter the same name as the compute name on the computer.

---

### 3. If your ISP checks the User ID

This authentication method is used mostly by ISPs providing RoadRunner services (for example, RR-TAS (Toshiba Authentication Service) or RR-Manager authentication). You must configure the service type, username and password exactly as provided by your ISP in SMT menu 4.

Menu 4 - Internet Access Setup

ISP's Name= MyISP

Encapsulation= Ethernet

Service Type= RR-Toshiba

My Login= cso@zyxel

My Password= \*\*\*\*\*

Retype to Confirm= N/A

Login Server= 0.0.0.0

IP Address Assignment= Dynamic

IP Address= N/A

IP Subnet Mask= N/A

Gateway IP Address= N/A

Network Address Translation= SUA Only

Field settings:

- g. **Service Type**: Select **RR-TAS** or **RR-Manager** authentication method used by your ISP.
- h. **Login Server**: Enter the IP address of the authentication server if you know it. Otherwise, leave this field to the default to have the P-2024 automatically obtain this information.
- i. **My Login Name**: Enter the login user name given to you by your ISP
- j. **My Password**: Enter the password associated with the login name.
- k. **WAN IP Address Assignment**: If the ISP did not assign you a fixed (or static) WAN IP address, select **Dynamic**, otherwise, select **Static**.
- l. **IP Address, Subnet Mask, Gateway IP Address**: If you select **Static** in the **WAN IP Address Assignment** field, enter the IP address, subnet mask and gateway device IP address provided by your ISP.

•

## Using Embedded Packet Trace

### Embedded Packet Trace

The P-2024 packet trace feature records and analyzes packets running on the LAN and WAN interfaces. It is designed for technical users who are interested in the details of the packet flow on the P-2024's LAN or WAN interface. It is also a diagnostic tool if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the packet trace result display is as follows:

Packet:

0    11880.160   ENET0-R[0062]   TCP   192.168.1.2:1108->192.31.7.130:80
--

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

There are two ways to view the trace result:

1. **Online Trace--display the trace real time on screen**
2. **Offline Trace--capture the trace first and display later**

The following details the trace commands in SMT menu 24.8.

### Online Trace

1. Trace LAN packet
2. Trace WAN packet

---

#### 1. Trace LAN packet

- 1.1 Disable WAN packet trace: **sys trcp channel enet1 none**
- 1.2 Enable LAN packet trace: **sys trcp channel enet0 bothway**
- 1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
- 1.4 Display brief online trace results: **sys trcd brief**

or

1.5 Display detailed online trace results: **sys trcd parse**

**Example:**

```
P-2024> sys trcp channel enet1 none
P-2024> sys trcp channel enet0 bothway
P-2024> sys trcp sw on
P-2024> sys trcl sw on
P-2024> sys trcd brief
  0   11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
  1   11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
  2   11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
  3   11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  4   11883.340 ENET0-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
  5   11883.610 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
  6   11883.620 ENET0-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
  7   11883.630 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
  8   11883.630 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  9   11883.650 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
 10   11883.650 ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
P-2024> sys trcd parse
---<0000>-----
LAN Frame: ENET0-RECV   Size:  62/  62   Time: 12089.790 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

Ethernet Header:
  Destination MAC Addr   = 00A0C5921311
  Source MAC Addr        = 0080C84CEA63
  Network Type           = 0x0800 (TCP/IP)

IP Header:
  IP Version              = 4
  Header Length           = 20
  Type of Service         = 0x00 (0)
  Total Length            = 0x0030 (48)
  Identification          = 0x330B (13067)
```

```
Flags                = 0x02
Fragment Offset      = 0x00
Time to Live         = 0x80 (128)
Protocol             = 0x06 (TCP)
Header Checksum      = 0x3E71 (15985)
Source IP            = 0xC0A80102 (192.168.1.2)
Destination IP       = 0xC01F0782 (192.31.7.130)
```

## TCP Header:

```
Source Port          = 0x045C (1116)
Destination Port     = 0x0050 (80)
Sequence Number      = 0x00BD15A7 (12391847)
Ack Number           = 0x00000000 (0)
Header Length        = 28
Flags                = 0x02 (....S.)
Window Size          = 0x2000 (8192)
Checksum             = 0xBEC3 (48835)
Urgent Ptr           = 0x0000 (0)
Options              =
    0000: 02 04 05 B4 01 01 04 02
```

## RAW DATA:

```
0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  ....L.c..E.
0010: 00 30 33 0B 40 00 80 06-3E 71 C0 A8 01 02 C0 1F  .03.@...>q.....
0020: 07 82 04 5C 00 50 00 BD-15 A7 00 00 00 00 70 02  ...\.P.....p.
0030: 20 00 BE C3 00 00 02 04-05 B4 01 01 04 02  ....
```

---<0001>-----

LAN Frame: ENETO-XMIT Size: 58/ 58 Time: 12090.020 sec

Frame Type: TCP 192.31.7.130:80->192.168.1.2:1116

## Ethernet Header:

```
Destination MAC Addr = 0080C84CEA63
Source MAC Addr      = 00A0C5921311
Network Type         = 0x0800 (TCP/IP)
```



## IP Header:

IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x002C (44)
Identification	= 0x57F3 (22515)
Flags	= 0x02
Fragment Offset	= 0x00
Time to Live	= 0xED (237)
Protocol	= 0x06 (TCP)
Header Checksum	= 0xAC8C (44172)
Source IP	= 0xC01F0782 (192.31.7.130)
Destination IP	= 0xC0A80102 (192.168.1.2)

## TCP Header:

Source Port	= 0x0050 (80)
Destination Port	= 0x045C (1116)
Sequence Number	= 0x4AD1B57F (1255257471)
Ack Number	= 0x00BD15A8 (12391848)
Header Length	= 24
Flags	= 0x12 (.A..S.)
Window Size	= 0xFAF0 (64240)
Checksum	= 0xF877 (63607)
Urgent Ptr	= 0x0000 (0)
Options	=

0000: 02 04 05 B4

## RAW DATA:

```
0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00  ...L.c.....E.
0010: 00 2C 57 F3 40 00 ED 06-AC 8C C0 1F 07 82 C0 A8  ..W.@.....
0020: 01 02 00 50 04 5C 4A D1-B5 7F 00 BD 15 A8 60 12  ...P.\J.....`.
0030: FA F0 F8 77 00 00 02 04-05 B4                    ...w.....
```

---&lt;0002&gt;-----

LAN Frame: ENET0-RECV Size: 60/ 60 Time: 12090.210 sec

Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

Ethernet Header:

Destination MAC Addr	= 00A0C5921311
Source MAC Addr	= 0080C84CEA63
Network Type	= 0x0800 (TCP/IP)

IP Header:

IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x0028 (40)
Identification	= 0x350B (13579)
Flags	= 0x02
Fragment Offset	= 0x00
Time to Live	= 0x80 (128)
Protocol	= 0x06 (TCP)
Header Checksum	= 0x3C79 (15481)
Source IP	= 0xC0A80102 (192.168.1.2)
Destination IP	= 0xC01F0782 (192.31.7.130)

TCP Header:

Source Port	= 0x045C (1116)
Destination Port	= 0x0050 (80)
Sequence Number	= 0x00BD15A8 (12391848)
Ack Number	= 0x4AD1B580 (1255257472)
Header Length	= 20
Flags	= 0x10 (.A....)
Window Size	= 0x2238 (8760)
Checksum	= 0xE8ED (59629)
Urgent Ptr	= 0x0000 (0)

TCP Data: (Length=6, Captured=6)

0000: 20 20 20 20 20 20

**RAW DATA:**

```
0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00 .....L.c..E.
0010: 00 28 35 0B 40 00 80 06-3C 79 C0 A8 01 02 C0 1F .(5.@...<y.....
0020: 07 82 04 5C 00 50 00 BD-15 A8 4A D1 B5 80 50 10 ...\.P....J...P.
0030: 22 38 E8 ED 00 00 20 20-20 20 20 20          "8....
```

## 2. Trace WAN packet

1.1 Disable LAN packet trace: **sys trcp channel enet0 none**

1.2 Enable WAN packet trace: **sys trcp channel enet1 bothway**

1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**

1.4 Display brief online trace results: **sys trcd brief**

or

1.5 Display detailed online trace results: **sys trcd parse**

### Example:

```
P-2024> sys trcp channel enet0 none
P-2024> sys trcp channel enet1 bothway
P-2024> sys trcp sw on
P-2024> sys trcl sw on
P-2024> sys trcd brief
0    12367.680 ENET1-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1    12370.980 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
2    12373.940 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
3    12374.930 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
4    12374.940 ENET1-T[0054] TCP 202.132.155.97:10261->192.31.7.130:80
5    12374.940 ENET1-T[0438] TCP 202.132.155.97:10261->192.31.7.130:80
6    12375.320 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
7    12375.360 ENET1-R[0090] UDP 202.132.155.95:520->202.132.155.255:520
P-2024> sys trcd parse
---<0000>-----
LAN Frame: ENET1-RECV   Size:1181/ 96   Time: 12387.260 sec
Frame Type: TCP 192.31.7.130:80->202.132.155.97:10270

Ethernet Header:
```

```

Destination MAC Addr    = 00A0C5921312
Source MAC Addr         = 00A0C5012345
Network Type            = 0x0800 (TCP/IP)

```

#### IP Header:

```

IP Version              = 4
Header Length           = 20
Type of Service         = 0x00 (0)
Total Length            = 0x048B (1163)
Identification          = 0xB139 (45369)
Flags                   = 0x02
Fragment Offset         = 0x00
Time to Live            = 0xEE (238)
Protocol                = 0x06 (TCP)
Header Checksum         = 0xA9AB (43435)
Source IP               = 0xC01F0782 (192.31.7.130)
Destination IP          = 0xCA849B61 (202.132.155.97)

```

#### TCP Header:

```

Source Port             = 0x0050 (80)
Destination Port        = 0x281E (10270)
Sequence Number         = 0xD3E95985 (3555285381)
Ack Number              = 0x00C18F63 (12685155)
Header Length           = 20
Flags                   = 0x19 (.AP..F)
Window Size             = 0xFAF0 (64240)
Checksum                = 0x3735 (14133)
Urgent Ptr              = 0x0000 (0)

```

#### TCP Data: (Length=1127, Captured=42)

```

0000: DF 33 AF 62 58 37 52 3D-79 99 A5 3C 2B 59 E2 78  .3.bX7R=y..<+Y.x
0010: A7 98 8F 3F A9 09 E4 0F-26 14 9C 58 3E 95 3E E7  ...?...&..X>.>.
0020: FC 2A 4C 2F FB BE 2F FE-EF D0  .*L/.../...

```

#### RAW DATA:

```

0000: 00 A0 C5 92 13 12 00 A0-C5 01 23 45 08 00 45 00 .....#E..E.
0010: 04 8B B1 39 40 00 EE 06-A9 AB C0 1F 07 82 CA 84 ...9@.....
0020: 9B 61 00 50 28 1E D3 E9-59 85 00 C1 8F 63 50 19 .a.P(...Y....cP.
0030: FA F0 37 35 00 00 DF 33-AF 62 58 37 52 3D 79 99 ..75...3.bX7R=y.
0040: A5 3C 2B 59 E2 78 A7 98-8F 3F A9 09 E4 0F 26 14 .<+Y.x...?....&.
0050: 9C 58 3E 95 3E E7 FC 2A-4C 2F FB BE 2F FE EF D0 .X>.>...*L/.../...

```

---<0001>-----

LAN Frame: ENET1-XMIT Size: 54/ 54 Time: 12387.490 sec

Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80

#### Ethernet Header:

Destination MAC Addr	= 00A0C5012345
Source MAC Addr	= 00A0C5921312
Network Type	= 0x0800 (TCP/IP)

#### IP Header:

IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x0028 (40)
Identification	= 0x7A0C (31244)
Flags	= 0x02
Fragment Offset	= 0x00
Time to Live	= 0x7F (127)
Protocol	= 0x06 (TCP)
Header Checksum	= 0x543C (21564)
Source IP	= 0xCA849B61 (202.132.155.97)
Destination IP	= 0xC01F0782 (192.31.7.130)

#### TCP Header:

Source Port	= 0x281E (10270)
Destination Port	= 0x0050 (80)
Sequence Number	= 0x00C18F63 (12685155)
Ack Number	= 0xD3E95DE9 (3555286505)
Header Length	= 20

Flags	= 0x10 (.A....)
Window Size	= 0x1DD5 (7637)
Checksum	= 0x7A12 (31250)
Urgent Ptr	= 0x0000 (0)

## RAW DATA:

```
0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00 ....#E.....E.
0010: 00 28 7A 0C 40 00 7F 06-54 3C CA 84 9B 61 C0 1F .(z.@...T<...a..
0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 10 ..(..P...c...].P.
0030: 1D D5 7A 12 00 00 ..Z...
```

---<0002>-----

LAN Frame: ENET1-XMIT Size: 54/ 54 Time: 12387.490 sec

Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80

## Ethernet Header:

Destination MAC Addr	= 00A0C5012345
Source MAC Addr	= 00A0C5921312
Network Type	= 0x0800 (TCP/IP)

## IP Header:

IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x0028 (40)
Identification	= 0x7B0C (31500)
Flags	= 0x02
Fragment Offset	= 0x00
Time to Live	= 0x7F (127)
Protocol	= 0x06 (TCP)
Header Checksum	= 0x533C (21308)
Source IP	= 0xCA849B61 (202.132.155.97)
Destination IP	= 0xC01F0782 (192.31.7.130)

## TCP Header:

Source Port	= 0x281E (10270)
-------------	------------------

```
Destination Port      = 0x0050 (80)
Sequence Number       = 0x00C18F63 (12685155)
Ack Number            = 0xD3E95DE9 (3555286505)
Header Length         = 20
Flags                 = 0x11 (.A...F)
Window Size           = 0x1DD5 (7637)
Checksum              = 0x7A11 (31249)
Urgent Ptr            = 0x0000 (0)
```

## RAW DATA:

```
0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00 ....#E.....E.
0010: 00 28 7B 0C 40 00 7F 06-53 3C CA 84 9B 61 C0 1F .({.@...S<...a..
0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 11 ..(..P...c...].P.
0030: 1D D5 7A 11 00 00                               ..Z...
```

P-2024&gt;

## Offline Trace

1. Trace LAN packet
2. Trace WAN packet

1. Trace LAN packet

- 1.1 Disable WAN packet trace: **sys trcp channel enet1 none**
- 1.2 Enable LAN packet trace: **sys trcp channel enet0 bothway**
- 1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
- 1.4 Wait for packets to pass through the P-2024 on the LAN
- 1.5 Disable trace logging: **sys trcp sw off** & **sys trcl sw off**
- 1.6 Display brief trace results : **sys trcp brief**
- 1.7 Display specific trace packets: **sys trcp parse <from\_index> <to\_index>**

### Example:

```
P-2024> sys trcp channel enet1 none
P-2024> sys trcp channel enet0 bothway
P-2024> sys trcp sw on
P-2024> sys trcl sw on
P-2024> sys trcp sw off
P-2024> sys trcl sw off
P-2024> sys trcp brief
```

```
0    10855.790 ENETO-T[0141] TCP 192.31.7.130:80->192.168.1.2:1102
1    10855.800 ENETO-R[0060] TCP 192.168.1.2:1102->192.31.7.130:80
2    10855.810 ENETO-R[0062] TCP 192.168.1.2:1103->192.31.7.130:80
3    10855.840 ENETO-R[0062] TCP 192.168.1.2:1104->192.31.7.130:80
4    10856.020 ENETO-T[0054] TCP 192.31.7.130:80->192.168.1.2:1102
```

```
5    10856.030 ENETO-T[0058] TCP 192.31.7.130:80->192.168.1.2:1103
```

```
6    10856.040 ENETO-R[0060] TCP 192.168.1.2:1103->192.31.7.130:80
```

```
P-2024> sys trcp parse 5 5
```

```
---<0005>-----
```

```
LAN Frame: ENETO-XMIT   Size:  58/  58   Time: 10856.030 sec
```

```
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1103
```

#### Ethernet Header:

```
Destination MAC Addr    = 0080C84CEA63
Source MAC Addr         = 00A0C5921311
Network Type            = 0x0800 (TCP/IP)
```

#### IP Header:

```
IP Version              = 4
Header Length           = 20
Type of Service         = 0x00 (0)
Total Length            = 0x002C (44)
Identification          = 0x7F02 (32514)
Flags                   = 0x02
```



```

Fragment Offset      = 0x00
Time to Live         = 0xED (237)
Protocol             = 0x06 (TCP)
Header Checksum      = 0x857D (34173)
Source IP            = 0xC01F0782 (192.31.7.130)
Destination IP       = 0xC0A80102 (192.168.1.2)

```

#### TCP Header:

```

Source Port          = 0x0050 (80)
Destination Port     = 0x044F (1103)
Sequence Number      = 0xD91B1826 (3642431526)
Ack Number           = 0x00AA405F (11157599)
Header Length        = 24
Flags                = 0x12 (.A..S.)
Window Size          = 0xFAF0 (64240)
Checksum             = 0xDCEF (56559)
Urgent Ptr           = 0x0000 (0)
Options              =

```

```
0000: 02 04 05 B4
```

#### RAW DATA:

```

0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00  ...L.c.....E.
0010: 00 2C 7F 02 40 00 ED 06-85 7D C0 1F 07 82 C0 A8  ,...@....}.....
0020: 01 02 00 50 04 4F D9 1B-18 26 00 AA 40 5F 60 12  ...P.O...&...@_`.
0030: FA F0 DC EF 00 00 02 04-05 B4                      .....

```

P-2024>

## 2. Trace WAN packet

- 1.1 Disable LAN packet trace: **sys trcp channel enet0 none**
- 1.2 Enable WAN packet trace: **sys trcp channel enet1 bothway**
- 1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
- 1.4 Wait for packets to pass through the P-2024 on the WAN
- 1.5 Disable trace logging: **sys trcp sw off** & **sys trcl sw off**

1.6 Display brief trace results: **sys trcp brief**

1.7 Display specific trace packets: **sys trcp parse <from\_index> <to\_index>**

**Example:**

```
P-2024> sys trcp channel enet0 none
P-2024> sys trcp channel enet1 bothway
P-2024> sys trcl sw on
P-2024> sys trcp sw on
P-2024> sys trcl sw off
P-2024> sys trcp sw off
P-2024> sys trcp brief
  0   12864.800 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
  1   12864.890 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
  2   12864.900 ENET1-T[0416] TCP 202.132.155.97:10282->204.217.0.2:80
  3   12865.120 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10278
  4   12865.130 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
  5   12865.220 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
P-2024> sys trcp parse 3 4
---<0003>-----
LAN Frame: ENET1-RECV   Size: 247/ 96   Time: 12865.120 sec
Frame Type: TCP 204.217.0.2:80->202.132.155.97:10278

Ethernet Header:
  Destination MAC Addr   = 00A0C5921312
  Source MAC Addr        = 00A0C5591284
  Network Type           = 0x0800 (TCP/IP)

IP Header:
  IP Version              = 4
  Header Length           = 20
  Type of Service         = 0x00 (0)
  Total Length            = 0x00E5 (229)
  Identification          = 0xE93B (59707)
  Flags                   = 0x02
  Fragment Offset         = 0x00
```

```

Time to Live           = 0xF0 (240)
Protocol               = 0x06 (TCP)
Header Checksum        = 0x6E15 (28181)
Source IP              = 0xCCD90002 (204.217.0.2)
Destination IP         = 0xCA849B61 (202.132.155.97)

```

**TCP Header:**

```

Source Port            = 0x0050 (80)
Destination Port       = 0x2826 (10278)
Sequence Number        = 0x4D713D8A (1299266954)
Ack Number             = 0x00C8C015 (13156373)
Header Length          = 20
Flags                  = 0x18 (.AP...)
Window Size            = 0x2238 (8760)
Checksum               = 0xAB57 (43863)
Urgent Ptr             = 0x0000 (0)

```

**TCP Data: (Length=193, Captured=42)**

```

0000: 48 54 54 50 2F 31 2E 31-20 33 30 34 20 4E 6F 74 HTTP/1.1 304 Not
0010: 20 4D 6F 64 69 66 69 65-64 0D 0A 44 61 74 65 3A Modified..Date:
0020: 20 57 65 64 2C 20 30 37-20 4A Wed, 07 J

```

**RAW DATA:**

```

0000: 00 A0 C5 92 13 12 00 A0-C5 59 12 84 08 00 45 00 .....Y....E.
0010: 00 E5 E9 3B 40 00 F0 06-6E 15 CC D9 00 02 CA 84 ...;@...n.....
0020: 9B 61 00 50 28 26 4D 71-3D 8A 00 C8 C0 15 50 18 .a.P(&Mq=....P.
0030: 22 38 AB 57 00 00 48 54-54 50 2F 31 2E 31 20 33 "8.W..HTTP/1.1 3
0040: 30 34 20 4E 6F 74 20 4D-6F 64 69 66 69 65 64 0D 04 Not Modified.
0050: 0A 44 61 74 65 3A 20 57-65 64 2C 20 30 37 20 4A .Date: Wed, 07 J

```

---<0004>-----

LAN Frame: ENET1-XMIT Size: 411/ 96 Time: 12865.130 sec

Frame Type: TCP 202.132.155.97:10278->204.217.0.2:80

**Ethernet Header:**

```

Destination MAC Addr   = 00A0C5591284

```

Source MAC Addr = 00A0C5921312  
Network Type = 0x0800 (TCP/IP)

## IP Header:

IP Version = 4  
Header Length = 20  
Type of Service = 0x00 (0)  
Total Length = 0x018D (397)  
Identification = 0xF20C (61964)  
Flags = 0x02  
Fragment Offset = 0x00  
Time to Live = 0x7F (127)  
Protocol = 0x06 (TCP)  
Header Checksum = 0xD59C (54684)  
Source IP = 0xCA849B61 (202.132.155.97)  
Destination IP = 0xCCD90002 (204.217.0.2)

## TCP Header:

Source Port = 0x2826 (10278)  
Destination Port = 0x0050 (80)  
Sequence Number = 0x00C8C015 (13156373)  
Ack Number = 0x4D713E47 (1299267143)  
Header Length = 20  
Flags = 0x18 (.AP...)  
Window Size = 0x1E87 (7815)  
Checksum = 0x4374 (17268)  
Urgent Ptr = 0x0000 (0)

## TCP Data: (Length=357, Captured=42)

0000: 47 45 54 20 2F 70 69 63-74 75 72 65 73 2F 6D 61 GET /pictures/ma  
0010: 67 61 7A 69 6E 65 5F 6C-6F 67 6F 2F 62 65 73 74 gazine\_logo/best  
0020: 6F 66 74 69 6D 65 73 2E-67 69 oftimes.gi

## RAW DATA:

0000: 00 A0 C5 59 12 84 00 A0-C5 92 13 12 08 00 45 00 ...Y.....E.

```
0010: 01 8D F2 0C 40 00 7F 06-D5 9C CA 84 9B 61 CC D9   ....@.....a..
0020: 00 02 28 26 00 50 00 C8-C0 15 4D 71 3E 47 50 18   ..(&.P....Mq>GP.
0030: 1E 87 43 74 00 00 47 45-54 20 2F 70 69 63 74 75   ..Ct..GET /pictu
0040: 72 65 73 2F 6D 61 67 61-7A 69 6E 65 5F 6C 6F 67   res/magazine_log
0050: 6F 2F 62 65 73 74 6F 66-74 69 6D 65 73 2E 67 69   o/bestoftimes.gi
P-2024>
```

## Debugging PPPoE Connection

### Debugging PPPoE Connection

---

You can use the packet trace tool on the P-2024 to troubleshoot PPPoE Internet connection. Follow the procedure below to perform packet trace for troubleshooting.

1. Remove the Ethernet cable from the LAN port on the P-2024
2. Enter the SMT through the console port
3. Enter SMT Menu 24.8-CI command mode
4. Type the following commands:
  - sys trcp sw on (turn on packet trace)
  - sys errctl 3 (save crash information and set the system to enter the mode after the crash)
  - poe debug 1 (turn on pppoe debug)
  - dev dial 1 (dial to remote node 1)
5. After you have entered the commands, you can send the saved logs in case your P-2024 crashes and there's nothing you can do to bring the connection up.
6. If the P-2024 crashes and you are able to enter the command mode, enter 'atds' in debug mode to display the logs. Copy the logs and send them to us.
7. If the P-2024 does not crash but you still can not dial out to your ISP for Internet connection. Capture the following logs. Copy the logs and send them to us.
  - sys trcp sw off (turn off packet trace)
  - sys log disp i (display system error logs)
  - sys trcp parse (display detailed trace results)

---

**Example- Trace Example on a crashed system**

```
ras> sys trcp sw on
ras> sys errctl 3
ras> poe debug 1
ras> dev dial 1
Start dialing for node <GPMI>...
poeNetCmdExe: chann poe0 event x420
poeChannDial: start session, peer<GPMI>
bdcastInit: pch poe0
poePut1SrvName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
bdcastSendInit: ll.pktTx() failed, pch poe0 ch enet0
poePut1SrvName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.....
poeI/C: ver 1 type 1 code x07 sessId x0000 len 274(x0112)
poeCtrlI/C: pkt len 274
poeGetTags()
service-name
service-name telstra
service-name bpa
service-name iprimus
service-name pacificinternet
service-name integrationisp
service-name bpa-dev
service-name bpa-sif
service-name telstrarna
service-name gpmsystems
service-name cmux
service-name launceston-broadband
```

```

service-name vivanet
service-name n1234567k00
service-name bigpond
service-name n7061992k
service-name n3068223k
service-name n2155202k
service-name n7061995k
AC-name vet1-exhibition-bsn-1
host-uniq 31303030 len 4
PADO recv'd, chann enet1
procPADO: for poe chann poe0
Chann poe0 sending request
poePut1SrvName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 12(x000C)
Undefined Address : 0xE3F045C4
Undefined Data : 0x56FF54FF
    r0= 0xE3F045C4    r1= 0x0001FFC0    r2= 0x000000E5    r3= 0x56FF54FF
    r4= 0xE3F045C4    r5= 0xE5BDBFEC    r6= 0x0001C468    r7= 0x60000093
    r8= 0x00000000    r9= 0xE3550000    r10=0xE3550000    fp= 0x00000000
    r12=0x56FF54FF    sp= 0x0001EDBC    lr= 0x00004F64    pc= 0x00013954
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
e5bdbfe0: e2 8f 00 06 e5 d5 20 06 e5 d5 20 0a e5 d5 20 0e ...b...f...j...n
e5bdbff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n

```

e5bdc0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n

e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n

Bootbase Version: V1.06 | 11/05/2004 19:29:47

RAM: Size = 8192 Kbytes

DRAM POST: Testing: 8192K

OK

FLASH: Intel 16M

ZyNOS Version: V3.60(MM.0) | 12/31/2004 13:39:02

Enter Debug Mode

atgo

(Compressed)

Version: RAS P2302RLP1, start: bfc58030

Length: 3DB3EC, Checksum: 9AA9

Compressed Length: 12AC58, Checksum: DC06

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

initialize ch =0, ethernet address: 00:A0:C5:CB:A8:16

initialize ch =1, ethernet address: 00:A0:C5:CB:A8:17

VC5402 Init...OK

Press ENTER to continue...

Enter Password : XXXX

## LAN/WAN Packet Trace

---

You can use the packet trace feature on the P-2024 to record and analyze packets transmitting through the LAN and WAN interfaces. It is designed for technical users who are interested in the details of the packet flow on the P-2024's LAN or WAN interface. It is also a very helpful diagnostic tool to solve Internet connection problems or if you want to know the details of a packet for configuring a filter rule.

The format of the result is displayed as follows:

Packet:



```
0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
```

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

There are two ways to display the trace results:

1. **Online Trace--display real-time trace results on the screen**
2. **Offline Trace-- save the trace results first and display them later**

The following shows you how to obtain and display the packet trace results in SMT menu 24.8 are as follows.

### Online Trace

1. Trace LAN packet
2. Trace WAN packet

1. Trace LAN packet

- 1.1 Disable capture the WAN packet trace: **sys trcp channel mpoa00 none**
- 1.2 Enable capture the LAN packet trace: **sys trcp channel enet0 bothway**
- 1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
- 1.4 Display brief online trace results: **sys trcd brief**
- or
- 1.5 Display detailed online trace results: **sys trcd parse**

### Example:

```

ras> sys trcp channel mpoa00 none
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> sys trcd brief
0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
1    11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
2    11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
3    11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80

```

```

4    11883.340 ENETO-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
5    11883.610 ENETO-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
6    11883.620 ENETO-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
7    11883.630 ENETO-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
8    11883.630 ENETO-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
9    11883.2602HW ENETO-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
10   11883.2602HW ENETO-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80

```

```

ras> sys trcd parse

```

```

---<0000>-----

```

```

LAN Frame: ENETO-RECV  Size: 62/ 62  Time: 12089.790 sec

```

```

Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

```

#### Ethernet Header:

```

Destination MAC Addr    = 00A0C5921311
Source MAC Addr         = 0080C84CEA63
Network Type            = 0x0800 (TCP/IP)

```

#### IP Header:

```

IP Version              = 4
Header Length           = 20
Type of Service         = 0x00 (0)
Total Length            = 0x0030 (48)
Identification          = 0x330B (13067)
Flags                   = 0x02
Fragment Offset         = 0x00
Time to Live            = 0x80 (128)
Protocol                = 0x06 (TCP)
Header Checksum         = 0x3E71 (15985)
Source IP               = 0xC0A80102 (192.168.1.2)
Destination IP          = 0xC01F0782 (192.31.7.130)

```

#### TCP Header:

```

Source Port             = 0x045C (1116)
Destination Port        = 0x0050 (80)
Sequence Number         = 0x00BD15A7 (12391847)

```

Ack Number = 0x00000000 (0)  
Header Length = 28  
Flags = 0x02 (....S.)  
Window Size = 0x2004 (8192)  
Checksum = 0xBEC3 (48835)  
Urgent Ptr = 0x0000 (0)  
Options =

0000: 02 04 05 B4 01 01 04 02

RAW DATA:

0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00 .....L.c..E.  
0010: 00 30 33 0B 40 00 80 06-3E 71 C0 A8 01 02 C0 1F .03.@...>q.....  
0020: 07 82 04 5C 00 50 00 BD-15 A7 00 00 00 00 70 02 ...\.P.....p.  
0030: 20 00 BE C3 00 00 02 04-05 B4 01 01 04 02 .....  
-----<0001>-----

LAN Frame: ENETO-XMIT Size: 58/ 58 Time: 12090.020 sec

Frame Type: TCP 192.31.7.130:80->192.168.1.2:1116

Ethernet Header:

Destination MAC Addr = 0080C84CEA63  
Source MAC Addr = 00A0C5921311  
Network Type = 0x0800 (TCP/IP)

IP Header:

IP Version = 4  
Header Length = 20  
Type of Service = 0x00 (0)  
Total Length = 0x002C (44)  
Identification = 0x57F3 (22515)  
Flags = 0x02  
Fragment Offset = 0x00  
Time to Live = 0xED (237)  
Protocol = 0x06 (TCP)  
Header Checksum = 0xAC8C (44172)  
Source IP = 0xC01F0782 (192.31.7.130)

Destination IP = 0xC0A80102 (192.168.1.2)

TCP Header:

Source Port = 0x0050 (80)

Destination Port = 0x045C (1116)

Sequence Number = 0x4AD1B57F (1255257471)

Ack Number = 0x00BD15A8 (12391848)

Header Length = 24

Flags = 0x12 (.A..S.)

Window Size = 0xFAF0 (2602HW40)

Checksum = 0xF877 (63607)

Urgent Ptr = 0x0000 (0)

Options =

0000: 02 04 05 B4

RAW DATA:

0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00 ...L.c.....E.

0010: 00 2C 57 F3 40 00 ED 06-AC 8C C0 1F 07 82 C0 A8 ..W.@.....

0020: 01 02 00 50 04 5C 4A D1-B5 7F 00 BD 15 A8 60 12 ...P.\J.....`.

0030: FA F0 F8 77 00 00 02 04-05 B4 ...w.....

---<0002>-----

LAN Frame: ENETO-RECV Size: 60/ 60 Time: 12090.210 sec

Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

Ethernet Header:

Destination MAC Addr = 00A0C5921311

Source MAC Addr = 0080C84CEA63

Network Type = 0x0800 (TCP/IP)

IP Header:

IP Version = 4

Header Length = 20

Type of Service = 0x00 (0)

Total Length = 0x0028 (40)

Identification = 0x350B (13579)

```

Flags                = 0x02
Fragment Offset      = 0x00
Time to Live         = 0x80 (128)
Protocol             = 0x06 (TCP)
Header Checksum      = 0x3C79 (15481)
Source IP            = 0xC0A80102 (192.168.1.2)
Destination IP       = 0xC01F0782 (192.31.7.130)

```

#### TCP Header:

```

Source Port          = 0x045C (1116)
Destination Port     = 0x0050 (80)
Sequence Number      = 0x00BD15A8 (12391848)
Ack Number           = 0x4AD1B580 (1255257472)
Header Length        = 20
Flags                = 0x10 (.A....)
Window Size          = 0x2238 (8760)
Checksum             = 0xE8ED (59629)
Urgent Ptr           = 0x0000 (0)

```

#### TCP Data: (Length=6, Captured=6)

```
0000: 20 20 20 20 20 20
```

#### RAW DATA:

```

0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  ....L.c..E.
0010: 00 28 35 0B 40 00 80 06-3C 79 C0 A8 01 02 C0 1F  .(5.@...<y.....
0020: 07 82 04 5C 00 50 00 BD-15 A8 4A D1 B5 80 50 10  ...\.P....J...P.
0030: 22 38 E8 ED 00 00 20 20-20 20 20 20          "8....

```

## 2. Trace WAN packet

1.1 Disable LAN packet trace: **sys trcp channel enet0 none**

1.2 Enable WAN packet trace: **sys trcp channel mpoa00 bothway**

1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**

1.4 Display brief online trace results: **sys trcd brief**

or

1.5 Display detailed online trace results: **sys trcd parse**

**Example:**

```

ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> sys trcd brief
0    12367.680 MPOA00-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1    12370.980 MPOA00-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
ras> sys trcd parse

```

```

---<0000>-----
LAN Frame: MPOA00-RECV  Size:1181/ 96  Time: 12387.260 sec
Frame Type: TCP 192.31.7.130:80->202.132.155.97:10270

```

**Ethernet Header:**

Destination MAC Addr	= 00A0C5921312
Source MAC Addr	= 00A0C5012345
Network Type	= 0x0800 (TCP/IP)

**IP Header:**

IP Version	= 4
Header Length	= 20
Type of Service	= 0x00 (0)
Total Length	= 0x048B (1163)
Identification	= 0xB139 (45369)
Flags	= 0x02
Fragment Offset	= 0x00
Time to Live	= 0xEE (238)
Protocol	= 0x06 (TCP)
Header Checksum	= 0xA9AB (43435)
Source IP	= 0xC01F0782 (192.31.7.130)
Destination IP	= 0xCA849B61 (202.132.155.97)

**TCP Header:**

Source Port	= 0x0050 (80)
Destination Port	= 0x281E (10270)

```

Sequence Number      = 0xD3E95985 (3555285381)
Ack Number           = 0x00C18F63 (12685155)
Header Length        = 20
Flags                = 0x19 (.AP..F)
Window Size          = 0xFAF0 (2602HW40)
Checksum             = 0x3735 (14133)
Urgent Ptr           = 0x0000 (0)

```

TCP Data: (Length=1127, Captured=42)

```

0000: DF 33 AF 62 58 37 52 3D-79 99 A5 3C 2B 59 E2 78  .3.bX7R=y..<+Y.x
0010: A7 98 8F 3F A9 09 E4 0F-26 14 9C 58 3E 95 3E E7  ...?...&..X>.>.
0020: FC 2A 4C 2F FB BE 2F FE-EF D0                      .*L/.../...

```

RAW DATA:

```

0000: 00 A0 C5 92 13 12 00 A0-C5 01 23 45 08 00 45 00  .....#E..E.
0010: 04 8B B1 39 40 00 EE 06-A9 AB C0 1F 07 82 CA 84  ...9@.....
0020: 9B 61 00 50 28 1E D3 E9-59 85 00 C1 8F 63 50 19  .a.P(...Y....cP.
0030: FA F0 37 35 00 00 DF 33-AF 62 58 37 52 3D 79 99  ..75...3.bX7R=y.
0040: A5 3C 2B 59 E2 78 A7 98-8F 3F A9 09 E4 0F 26 14  .<+Y.x...?...&.
0050: 9C 58 3E 95 3E E7 FC 2A-4C 2F FB BE 2F FE EF D0  .X>.>...*L/.../...

```

## Offline Trace

1. Trace LAN packet
2. Trace WAN packet

1. Trace LAN packet

- 1.1 Disable WAN packet trace: **sys trcp channel mpoa00 none**
- 1.2 Enable LAN packet trace: **sys trcp channel enet0 bothway**
- 1.3 Enable trace logging: **sys trcp sw on** & **sys trcl sw on**
- 1.4 Wait for packets to pass through the P-2024 on the LAN
- 1.5 Disable trace logging: **sys trcp sw off** & **sys trcl sw off**

1.6 Display brief trace results: `sys trcp brief`

1.7 Display specific packet trace results: `sys trcp parse <from_index> <to_index>`

## 2. Trace WAN packet

1.1 Disable LAN packet trace: `sys trcp channel enet0 none`

1.2 Enable WAN packet trace: `sys trcp channel mpoa00 bothway`

1.3 Enable trace logging: `sys trcp sw on` & `sys trcl sw on`

1.4 Wait for packets to pass through the P-2024 on the WAN

1.5 Disable trace logging: `sys trcp sw off` & `sys trcl sw off`

1.6 Display brief trace results: `sys trcp brief`

1.7 Display specific packet trace results: `sys trcp parse <from_index> <to_index>`

## CLI Command List

The most updated CI command list is available in the release notes with every ZyXEL firmware release. Download the latest firmware package (\*.zip), from ZyXEL's public WEB site at <http://www.zyxel.com/support/download.php>. You must unzip the package to get the release note in PDF format.